

# LANGATTOMUUS OSANA YRITYKSEN VOIP-JÄRJESTELMÄÄ

LAHDEN AMMATTIKORKEAKOULU  
Tekniikan ala  
Tietotekniikka  
Tietoliikennetekniikka  
Opinnäytetyö  
Kevät 2010  
Ella Lerkki

Lahden ammattikorkeakoulu  
Tietotekniikan koulutusohjelma

LERKKI, ELLA: Langattomuus osana yrityksen VoIP-järjestelmää

Tietoliikennetekniikan opinnäytetyö, 55 sivua, 4 liitesivua

Kevät 2010

TIIVISTELMÄ

---

Tämän opinnäytetyön tavoitteena on löytää sopivin ratkaisumalli, jolla siirtyminen kiinteästä VoIP:sta mobiilimpaan ympäristöön A-lehdet Oy:ssä voidaan toteuttaa.

Opinnäytetyön tarkoituksena on tutkia VoIP-tekniikka yleensä sekä langattoman siirtotien tuomia haasteita tekniikalle. Tutkimusympäristönä on A-lehtikonsernin verkkoinfrastruktuuri sekä käyttäjäkunta. Työtä varten tehtiin käyttäjä tutkimuksia eri käyttäjäryhmille ja näiden pohjalta tutkittiin, missä määrin siirtyminen on tarpeellista.

VoIP on tekniikka, jota käyttäen voidaan siirtää ääntä reaaliaikaisesti IP-verkon ylitse. VoIP-tekniikka koostuu erilaisista standardeista, joiden avulla voidaan suorittaa puheen signalointi, istunnon luominen, laadun varmentaminen sekä varmistua liikennöinnin turvallisuudesta.

Langattoman VoIP-tekniikan tuomia hyötyjä käyttäjälle ovat tehokkuus ja mobiilius. Langaton VoIP eroaa perinteisestä siinä, että langaton siirtotie vaatii lisäksi useita määrittelyjä QoS:n, tietoturvan, tiedon eheyden ja käyttäjien tunnistuksen sekä handoffien toteuttamiseksi ja näiden kaikkien toiminnan varmistamiseksi.

Ratkaisuksi esitetään SIP-protokollan käyttämistä signaloinnissa, sillä se mahdollistaa liikennöinnin ulkoverkkoon NAT:n ylitse. Käytössä olevan Cisco Systemsin VoIP-järjestelmän hallintaohjelmisto tulee päivittää sellaiseksi, että vanhentuneiden laitteiden lisenssit voidaan ottaa uudelleen käyttöön. Mobiiliuden tuomiseksi A-lehtien VoIP-ympäristöön, tulee olemassa olevan langattoman verkon kapasiteetti kartoittaa optimaaliseksi, jonka lisäksi data- ja ääniliikenne tulee erottaa toisistaan erillisiin virtuaalisiin verkkoihin.

Avainsanat: VoIP, WLAN, handoff, SIP, H.323, Cisco, QoS, security, NAT

Lahti University of Applied Sciences  
Degree Programme in information technology

LERKKI, ELLA:

Wireless VoIP system

Bachelor's Thesis in telecommunications, 55 pages, 4 appendices

Spring 2010

ABSTRACT

---

This thesis deals with VoIP technology in general and analyzes the challenges that wireless media bring along. The aim of the thesis was to find the most suitable solution to implement the transition from A-lehdet Oy's existing VOIP system to a more mobile environment.

The research environment is A-lehdet Oy's network infrastructure and its users. User studies were made to different groups of users to estimate the number of users that need mobility.

Using VoIP technology, voice can be transmitted in real-time through IP networks. VoIP technology consists of different standards which handle voice-signaling, create sessions, confirm quality services and standards, and make sure that data is transmitted securely.

The benefits that wireless VoIP technology brings to its users are efficiency and mobility. Wireless VoIP differs from traditional VoIP in its need to have more specific specifications for QoS, security, integrity of data, user authentication and for handoff processes.

The solution offered in the thesis, is to use the SIP protocol in call-signaling due to its feature that makes it possible to transfer data to an outer network through NAT. Cisco Systems' VoIP system controller program currently used by A-lehdet needs to be updated into such a version that allows the outdated licenses to be reused. In the process of bringing mobility to A-lehdet's VoIP environment, it is essential that the existing wireless network will be optimized and that data and voice transmissions will be divided into separate virtual networks.

Key words: VoIP, WLAN, handoff, SIP, H.323, Cisco, QoS, security, NAT

## LYHENNELUETTELO

802.11	Standardi langattomalle lähiverkolle, WLAN:lle. IEEE:n vuonna 1997 ratifioima. 802.11-työryhmät vastaavat langattoman verkon eri osa-alueista.
802.11a, b, g, n	Langattoman verkon 4 eri versiota. 802.11b ja g toimivat 2,4 GHz:n taajuudella ja 802.11a toimii 5 Ghz:n taajuudella. 802.11n toimii kummallakin taajuudella.
802.11e	IEEE:n langattoman verkon standardin laajennus määrittelemään verkon QoS-ominaisuuksia.
802.11i	IEEE:n langattoman verkon standardin laajennus määrittelemään verkon tietoturvaominaisuuksia.
802.11r	IEEE:n lisälaajennus langattoman verkon handoff-toimintoihin.
802.11u	WIEN (Wireless Interworking with External Networks) on IEEE:n lisämäärittely langattomasta verkosta mobiiliverkkoon siirtymiselle.
802.11q	IEEE:n standardi virtuaaliselle lähiverkolle.
802.1x	IEEE:n standardi porttipohjaiselle autentikoinnille, jossa autentikaation osallistuu tukiasema, tunnistautumispalvelin ja liittyvä laite.
AAA	Authentication, Authorozation and Accounting on käyttäjätunnistusperiaate, jossa käyttäjä autentikoidaan, tämän oikeudet todennetaan ja käyttäjätietoja tilastoidaan.
AES	Advanced Encryption Standard on lohkosalausstandardi, jossa on käytössä Rijndael-salausmenetelmä.
CCMP	Counter Mode with Cipher Block Changinfg Message Authentication Protocol on osa 802.11i-standardia ja yksi langattoman verkon salausprotokolla.
COPS	Common Open Policy Server on yksinkertainen haaste-vastausprotokolla, jota voidaan käyttää jakamaan verkossa policy-tietoja serveriltä clienteleille.

CoS	Class Of Service on kokoelma QoS-protokollia, joka toimii OSI-mallin datalinkkikerroksella.
CRC	Cyclic Redundancy Check on tiivistealgoritmi, jota käytetään tarkistamaan liikennöidyn datan eheys.
CSMA/CA	Carrier Sensible Multiple Access with Collision Avoidance on langattoman verkon vuoronvarausmenetelmä, jossa lähetetään dataa vain silloin kun media on vapaa.
DFC	Distributed Coordination Function on CSMA/CA-menetelmän pohjalla toimiva mekanismi langattomaan verkkoon pääsyn hallintaan.
DiffServ	Differentiated Services on IETF:n määrittelemä, Internetille tarkoitettu palvelunlaatumekanismi liikenteen hallintaan.
DoS	Denial Of Service on palvelunestohyökkäys, jolla pyritään lamauttamaan verkon toiminta.
DSCP	DiffServ Code Points on 6-bittinen tieto IP-paketin header-tietueessa. DSCP:ssä ilmoitetaan tieto paketin luokasta erilaisin määrittäksin.
EAP	Extensible Authentication Protocol on IETF:n määrittelemä käyttäjien tunnistusprotokolla, joka on yhteensopiva 802.1x-standardin kanssa.
EAPoW	EAP Over WLAN on EAP-sovitin langattoman verkon käyttäjien autentikointiin.
EDCA	Enhanced Distributed Channel Access on IEEE:n 802.11e-standardin käyttämä menetelmä luoda priorisoitu yhteys sovellusten välille.
H.255	H.323:n alamäärittäminen RAS (Registration, Admission and Status), joka määrittelee multimediapuhelun signaloinnin sekä hallinnoi rekisteröintiä, pääsyä ja istunnon tilaa.
H.245	H.323:n alamäärittäminen, joka määrittelee multimediaistunnon hallinnan.
H.248	H.248 eli Megaco (Media Gateway Control Protocol) on määrittäminen operaattoriverkoissa liikennöitävien multimediastreamien hallintaan.

H.323	ITU-T:n standardimäärittely, joka määrittelee komponentit multimediaistunnoille.
IDS	Intrusion Detection System on järjestelmä, jolla voidaan valvoa verkon liikennettä ja havaita mahdolliset tunkeutajat.
IP	Internet Protocol on pakettikytkentäinen tiedonsiirtomenetelmä.
LEAP	Light Extensible Authentication Protocol on Ciscon 802.1x-protokollan laillisuustarkistustoteutus, joka toteutetaan haaste-vastausmenetelmällä sekä dynaamisilla salausavaimilla.
MAN	Metropolitan Area Network on yleensä runkoverkkotyyppinen alueverkko, joka kattaa esimerkiksi yhden kaupungin alueen.
MD5	Message Digest 5 on kryptografinen tiivistefunktio, jota käytetään mm. EAP-autentikoinnissa tarkistamaan käyttäjän oikeellisuus.
MPLS	Multiprotocol Label Switching on IP-pakettien liikennöintiin nopeissa operaattorirunkoverkoissa käytettävä menetelmä.
NAT	Network Addressing Translation on osoitteenmuunnosmenetelmä, jonka avulla voidaan piilottaa julkisesti liikennöidyt osoitteet sisäverkossa ja päinvastoin.
OSI	Open System Interconnection tarjoaa mallin, jonka avulla voidaan eri tiedonsiirtoprotokollat jakaa seitsemään eri kerrokseen.
PBX	Private Branch Exchange on käsite, jota käytetään yksityisestä puhelinvaihteesta.
PEAP	Protected Extensible Authentication Protocol on Ciscon ja RSA Securityn tukema luonnos IETF-standardiksi, PEAP edellyttää TLS-sertifikaattia RADIUS-palvelimessa.
Q.931	ITU-T:n suositus ISDN-yhteyksien muodostamiseen ja hallintaan.

QoS	Quality of Service on tietoverkoissa käytetty menetelmä, jolla pyritään takaamaan tiedonsiirron laatu erilaisten luokittelujen ja priorisoinnin avulla.
RSN	Robust Security Network on IEEE:n 802.11i-standardin käsite, joka kokoaa eri tietoturvamääräykset yhteen. RSN käyttää AES-salausta, 802.1x:n sekä EAP:n kanssa.
RSSI	Received Signal Strength Indication on signaalitason mittari tietoliikenneympäristöissä.
RSVP	Resource Reservation Protocol on kuljetuskerroksen protokolla, jota käytetään resurssien varaukseen.
RTCP	Real-time Transport Control Protocol on RTP-protokollan rinnalla toimiva asetus. RTCP kerää ja analysoi sekä lähettää tietoa RTP-istunnosta.
RTP	Real-time Transport Protocol määrittelee pakettimuodon multimedialähetysille ja kuljettaa paketit IP-verkossa.
SCCP	Skinny Call Control Protocol on Cisco Systemsin määrittelemä protokolla mediastream-lähetysille Call Manager-ympäristössä.
SDP	Session Description Protocol on IETF:n protokolla mediastream-istuntoja kuvailevien parametrien määrittelylle.
SIP	Session Initiation Protocol on signaalointiprotokolla, jota käytetään multimediaistunnoissa, liikennöitäessä ääntä tai videota IP-verkossa.
SIP URI	SIP Uniform Resource Identifier on SIP-istunnoissa käyttäjiä yksilöivä tietue.
SPIT	Spam Over Internet Technology on ns. VoIP Spam.
STUN	Simple Traversal of UDP Through Network Address Translation on menetelmä, jota voidaan käyttää liikennöitäessä NAT:n lävitse UDP:llä.

TCP	Transmission Control Protocol on yhteydellinen kuljetuskerroksen protokolla, joka takaa luotettavan lähetyksen sekä tarkastaa pakettien saapumisjärjestyksen.
TKIP	Temporary Key Integrity Protocol on langattomien lähiverkkojen tietoturvaprotokolla ja WEP-protokollan seuraaja.
TLS	Transport Layer Security on salausprotokolla, jota käytetään mm. suojaamaan www-sivustojen tiedonsiirtoa.
ToS	Type of Service on Ipv4-osoitteen header-tietueen 8-bittinen tyyppimääre.
UDP	User Datagram Protocol on yhteydetön kuljetuskerroksen tiedonsiirtoprotokolla, joka ei varmista paketin perille menoa. UDP on tiedonsiirrossa nopeampi menetelmä kuin yhteydellinen TCP.
VLAN	Virtual Local Area Network eli virtuaalinen lähiverkko on lähiverkon osa, joka saattaa olla fyysisesti eri lokaatiossa, mutta on loogisesti osa lähiverkkoa.
VoIP	Voice Over IP on tekniikka, jolla voidaan toteuttaa reaaliaikaisia puheluita ja videopuheluita IP-verkossa.
VPN	Virtual Private Network on menetelmä, jolla voidaan yhdistää kaksi tai useampi verkko julkisen verkon yli näennäisesti samaksi verkoksi.
WEP	Web Equivalent Privacy on IEEE:n 802.11-standardin ensimmäinen salausmenetelmä, joka kehitettiin langattoman verkon liikenteen suojaksi.
WLAN	Wireless Local Area Network on käsite, jolla tarkoitetaan langatonta lähiverkkoa.
WPA	Wi-Fi Protected Access on IEEE:n 802.11i-standardin määrityksiä sisältävä menetelmä, joka kehitettiin korvaamaan edeltäjänsä, WEP:n heikkouksia.
WPA-2	WPA-2 on langattomien 802.11-verkkojen viimeisin tietoturvamääritys



# SISÄLLYS

1 JOHDANTO.....	1
2 VOIP – ÄÄNTÄ JA VIDEOA IP-VERKOISSA.....	2
2.1 VoIP:n tekniikka ja verkkoinfrastruktuuri.....	2
2.2 VoIP-järjestelmän toiminta OSI-mallissa .....	3
2.3 VoIP-verkon laitteet - Media Gateway, Gateway Controller ja Call Manager.....	5
2.4 QoS ja sen tärkeys VoIP-järjestelmälle.....	6
2.5 VoIP-järjestelmän tietoturvasta ja tietoturvaratkaisuista.....	8
2.6 VoIP-tekniikan tuomat palvelut yrityksille.....	9
3 VOIP:N SIGNALOINTIPROTOKOLLAT .....	10
3.1 SIP - Session Initiation Protocol.....	10
3.1.1 SIP-istunto .....	12
3.1.2 SIP ja NAT .....	14
3.2 H.323 15	
3.2.1 H.323-istunto.....	16
3.2.2 H.323:n tunnelointi NAT:n läpi.....	18
3.3 Muita signaalointiprotokollia.....	18
4 KOHTI LANGATONTA JÄRJESTELMÄÄ.....	20
4.1 VoIP ja langaton siirtotie.....	20
4.1.1 Liikenteen priorisointi.....	21
4.1.2 802.11e – QoS-määritykset langattomalle verkolle.....	22
4.2 802.11i-standardi ja VoWLAN-järjestelmän tietoturvallisuus määrittelyt.....	23
4.2.1 WPA-2 ja sitä edeltäneet tietoturvaprotokollat .....	24
4.2.2 EAP – protokolla käyttäjien autentikointiin.....	25

4.3 Handoff-operaatio – joustavuutta mobiiliuuteen .....	26
4.3.1 Langattomien tukiasemien väliset handoff-operaatiot.....	27
4.3.2 Siirtyminen WLAN:sta GSM-verkkoon.....	28
4.4 Nokia Call Connect for Cisco.....	32
5 VARAUTUMINEN TULEVAISUUTEEN.....	34
6 MEDIATALO A-LEHDET .....	36
6.1 A-lehdet Oy.....	36
6.2 A-lehtitalo Helsingin Kulosaarissa.....	36
6.2.1 A-lehtien lähiverkko ja laitteet.....	37
6.2.2 A-lehtien langattomat verkot ja niiden resurssit.....	37
6.3 Puhelinmyyntitoimistot ja Soundin toimitus .....	38
7 KÄYTTÄJÄTUTKIMUKSIA JA NIIDEN TULOKSIA.....	40
7.1 Käyttäjäkyselyn tuloksia puhelinmyyntikonttoreista.....	41
7.2 Käyttäjäkyselyn tuloksia pääkonttorilta.....	42
8 SKENAARIOITA .....	44
8.1 Käyttöönotto puhelinkonttoreiden esimiehille ja yhteyshenkilöille	44
8.2 Langattomuutta tarvitsevat käyttäjät – tehokkuutta työntekoon.....	45
8.3 Koko yrityksen muuttaminen langattomaan VoIPpiin.....	45
8.4 Ratkaisujen toteuttaminen.....	46
8.5 Siirtymän hyödyt ja haitat vastakkain.....	48
9 YHTEENVETO.....	49
LÄHTEET.....	51
LIITTEET .....	56

# 1 JOHDANTO

Opinnäytetyössä on tarkoitus tutkia VoIP-tekniikkaa ja langattoman verkon haasteita langattomalle VoIP-järjestelmälle. Työssä käsitellään yleisesti VoIP-tekniikan ja järjestelmän toimintaa sekä tutkitaan, mitä mahdollisuuksia ja haasteita radiotie siirtomedia tuo järjestelmän toimintaan.

Tutkimustyön pohjana ovat A-lehdet Oy:n tämänhetkinen käyttäjäkunta sekä verkkoinfrastruktuuri. Työn tavoitteena on kartoittaa A-lehtitalon ja sen ulkoisten toimipisteiden VoIP-järjestelmän nykytilaa, käyttäjien tarpeita sekä tutkia järjestelmän laajentamismahdollisuuksia.

Työn tutkimusongelmana on selvittää, miten langaton VoIP-järjestelmä kannattaa ottaa käyttöön A-lehdissä ja missä mittasuhteissa sen toteuttaminen olisi yrityksen ja käyttäjien kannalta järkevintä. Tämän opinnäytetyön tavoitteena on löytää sopivin tekniikka ja tapa toteuttaa mahdollinen siirtymä langattomaan VoIP:aan A-lehtien nykyisen verkkoinfrastruktuurin rinnalle sekä kartoittaa mahdollisen siirtymän tuomat hyödyt ja haitat yritykselle.

## 2 VOIP – ÄÄNTÄ JA VIDEOA IP-VERKOISSA

Voice over Internet Protocol eli VoIP on yleinen määritelmä tekniikalle, jossa pakettikytkentäisissä, IP-pohjaisissa verkoissa liikennöidään digitalisoitua reaaliaikaista ääntä, videokuvaa ja dataa. VoIP-järjestelmien laitteet, perinteisiin puhelinjärjestelmiin verrattuna, tarjoavat monipuolisempia toimintoja ja ovat edeltäjiään edullisempia pitkällä aikavälillä. (Wallingford 2005, 8.)

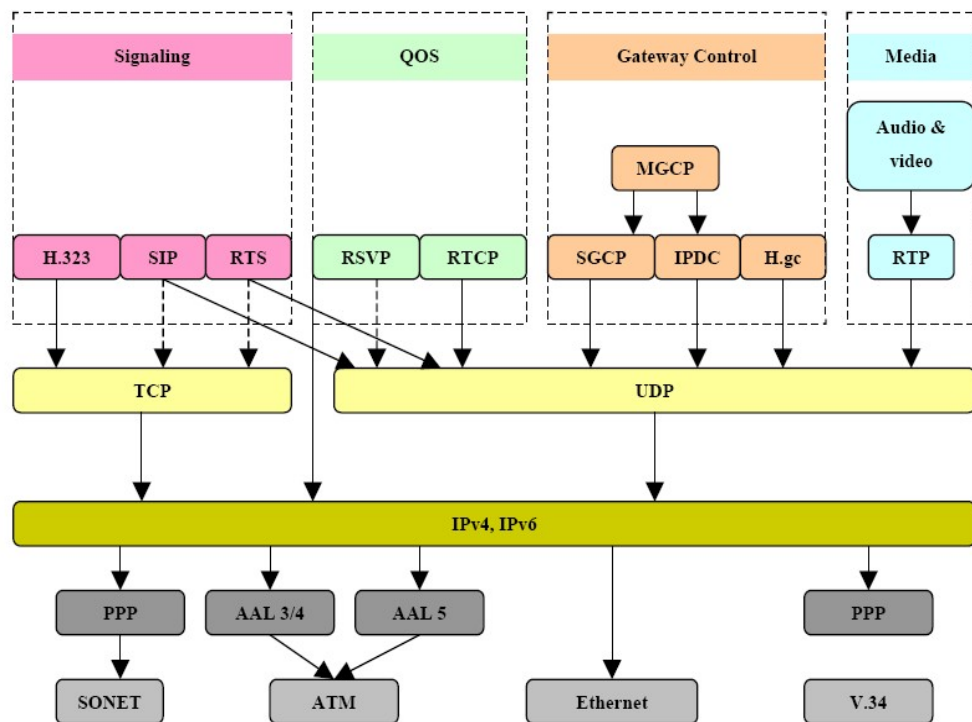
VoIP-järjestelmässä verkko- ja päätelaitteiden etähallinta onnistuu keskitetysti mutkattomammin kuin aiemmin. IP-verkoissa myös toipuminen linjojen rikkoutumisesta on perinteisiä puhelinverkkoja parempi verkon TCP/IP-protokollaperheen (Transmission Control Protocol / Internet Protocol) uudelleen reitittymisominaisuuksien ansiosta. (Wallingford 2005, 8.)

VoIP-tekniikan tuomat monipuolisemmat palvelut kasvattavat myös siirtomedian ja verkon vaatimuksia. Sen lisäksi, että IP-verkossa liikennöidään normaalia dataa, tulee myös huomioida ja priorisoida siirrettävä multimedialiikenne. (Wallingford 2005, 13 - 14.)

### 2.1 VoIP:n tekniikka ja verkkoinfrastruktuuri

Ethernet on yksi eniten käytettyjä lähiverkkotekniikoita, joissa VoIP-järjestelmä voidaan ottaa käyttöön. VoIP-järjestelmä voidaan rakentaa jo olemassa olevaan lähiverkkoon tai sen rinnalle ja verkkoa on helppo laajentaa käytön kasvaessa. OSI-mallin (Open Systems Interconnection) kerrosten protokollakuvan avulla (KUVIO 1) voidaan VoIP:ssa käytettyjä protokollia tutkia jäsennetymmin. (Hyttinen 2001.)

Neljän alimman kerroksen protokollat ovat kuin missä tahansa IP-pohjaisessa verkossa; eroavaisuudet tulevat esille vasta siirryttäessä kuljetuskerroksen yläpuolelle. Ylemmillä tasoilla toimivat VoIP-liikenteen signaalointiprotokollat, palvelun laadun takaavat QoS (Quality of Service) -protokollat sekä reaaliaikaiset lähetykset mahdollistava Real-time Transfer Protocol (RTP). (Hyttinen 2001.)



KUVIO 1. Internet Multimedia Protokolla-pino OSI-mallissa (Hyttinen 2001)

## 2.2 VoIP-järjestelmän toiminta OSI-mallissa

Alimmilla kerroksilla, fyysisellä ja datalinkki kerroksella, määritellään siirtomediaalle sen fyysiset ja elektroniset standardit. Datalinkkikerroksella hoidetaan osittain myös dataliikenteen virheenkorjausta kehystämällä datapaketit ja tarkistamalla datan eheys CRC-bittien avulla. (Wallingford 2005, 15 - 16.)

OSI-mallin kolmannella kerroksella, verkkokerroksella, määritellään liikennöitävän datan reititys, yhteyksien luonti, ylläpito ja purkaminen. Verkkokerrosta ylemmältä, kuljetuskerrokselta, tulevat datakehykset paketoidaan, osoitteistetaan ja siirretään eteenpäin. (Wallingford 2005, 13 - 14.)

Verkkokerros on VoIP-järjestelmässä ylin kerros, jonka toiminta on verkon kannalta kriittistä. Koska VoIP:ssa osoitteistus ja liikenteen ohjaus perustuu laitteiden Mac- ja IP-osoitteisiin, sovellusten tulee osata osoittaa verkkokerrokselle ja siellä määriteltäviin osoitteisiin, jotta liikennöinti verkossa olisi mahdollista. (Wallingford 2005, 13 - 14.)

Kuljetuskerroksella määritellään, käytetäänkö yhteydessä yhteydellistä vai yhteydetöntä tiedonsiirtoa. Yhteydellistä, TCP:tä (Transmission Control Protocol) käytetään neuvottelemaan yhteys päätelaitteiden ja näiden välissä olevien verkkolaitteiden välille. TCP:tä käytetään liikennöimään virheille herkkää puhelu-signaalintidataa sekä tarvittaessa myös pienentää tai kasvattaa ikkunakokoa. Ikkunan kokoa muuttamalla voidaan hallita sitä, kuinka paljonko dataa vastaanottaja yhdellä kertaa vastaanottaa. TCP-lähetys varmistaa, että vastaanottava osapuoli saa lähettäjän lähettämän datan SYN-, ACK- ja FIN-viesteillä, joita siirretään koko yhteyden voimassaolon ajan. (Wallingford 2005, 13 - 14.)

VoIP-puheyhteyden liikenne suoritetaan ilman jatkuvaa yhteyttä UDP-protokollalla (User Datagram Protocol), sillä ääniliikenteelle IP-verkossa riittää 'best effort'-malli. UDP:tä voidaan käyttää siis siksi, ettei puheluliikenteessä ole tarpeen varmistaa, meneekö jokainen paketti perille. UDP:n käyttö tiedonsiirrossa mahdollistaa nopeamman tiedonsiirron. (Wallingford 2005, 13 - 14.)

RSVP:llä (Resource reservation protocol) hallitaan kuljetuskerroksella siirtomedian resursseja. Kuljetuskerroksella määritetään lisäksi RTP:n (Real-time Transport Protocol) avulla standardoitu, istuntokohtaisesti sovittava, paketointimalli reaaliaikaisen datan kuljettamiselle internetissä. Yhden VoIP-puhelun aikana on käynnissä kaksi yksisuuntaista, sovitun RTP:n mukaista

istuntoa, joista toinen kuljettaa puheen tai videon ja toinen signaalintidatan. RTCP:n (Real-time Transport Control Protocol) avulla tarkkaillaan RTP:n toimintaa ja keräävät tietoa lähetetyn datan laadusta. (Hyttinen 2001.)

Istuntokerroksen signaalointia määritteleviä protokollia ovat SIP (Session Initiation Protocol), H.323, SCCP (Skinny Call Control Protocol), MGCP (Media Gateway Control Protocol) ja Megaco (Media Gateway Control Protocol) eli H.248, joita tutkitaan tarkemmin luvussa kolme. (Hyttinen 2001.)

Kahdella ylimmällä kerroksella, esitystapa- ja sovelluskerroksella, tapahtuu datan muuntaminen haluttuun tiedostomuotoon erilaisilla kodekeilla. Kaksi ylintä kerrosta vastaavat myös konkreettisesta kanssakäymisestä käyttäjän kanssa ohjelma- ja hallintarajapinnoilla. (Wallingford 2005, 18 - 19.)

## 2.3 VoIP-verkon laitteet - Media Gateway, Gateway Controller ja Call Manager

VoIP-verkko koostuu pääosin samanlaisista komponenteista kuin perinteinen piirikytkentäinen verkko, sillä erotuksella, että liikennöinti tapahtuu eri tekniikalla. VoIP-verkon kolmena pääelementtinä pidetään datan liikennöinnistä vastaavaa IP-verkkoa päätelaitteineen, Media gatewaytä sekä tämän kontrolleria, jotka vastaavat signaalien konvertoimisesta sopivaksi siirtotielle.

(VoIP Network Components 2009.)

Media gatewaytä voidaan kuvailla rajapinnaksi, joka huolehtii siitä, että siirrettävä ääni- tai videosignaali voidaan kuljettaa IP-verkossa ja toisaalta piirikytkentäiseen puhelinverkkoon voidaan liikennöidä paketteja. Gatewaytä käytetään siis muuntamaan lähetettävä data sopivaksi sen kohdeverkkoon.

(VoIP Network Components 2009.)

Media gateway huolehtii puhelujen välittämisestä ja niiden tunnistamisesta. Näiden lisäksi media gateway vastaa signaalien konvertoimisesta analogisesta digitaalseksi ja päinvastoin sekä äänitiedostopakettien luonnista kodekkien, esimerkiksi kompressoimattoman G.711:n, avulla. (VoIP Network Components 2009.)

Media Gateway Controller eli Call Agent vastaa puhelujen välittämisestä verkkojen välillä MGCP:llä. Controller keskustelee gatewayden kanssa viesteillä, jotka sisältävät istunnon otsikon, sen parametrit ja kuvauksen. Media gatewayn ja kontrollerin välinen liitäntä toteutetaan MECAGO-protokollalla. (Hytinen 2001.)

Call Manager, joka tunnetaan myös Cisco Unified Communications Managerina, on Cisco Systemssin tuotteilleen tarjoama hallintaympäristö. Call Manager-versioista uusin tulokas on 8.0. Call Manager-ohjelmiston avulla voidaan hallita keskitetysti VoIP-puhelimia, puheluliikenteelle tarkoitettua gatewaytä sekä erilaisia multimediasovelluksia. (Cisco Systems 2004.)

## 2.4 QoS ja sen tärkeys VoIP-järjestelmälle

QoS:n eli Quality of Servicen tukijalkana on hyvä verkon liikenteen ja verkon resurssien suunnittelu. Suunnittelijan tulee toteuttaa riittävästi kaistaa tarjoava sekä järjestelmällinen verkkoinfrastruktuuri organisaation sisällä sekä sisäverkosta ulospäin. Eri verkkoprotokollien ja näiden ominaisuuksien avulla toteutetaan kaistanvaraus, käyttäjien priorisointi ja laadunvalvonta sekä kontrolloidaan verkkoa, sen resursseja ja pyritään vähentämään kaistalla esiintyviä häiriöitä. Yleisiä häiriötekijöitä ovat viive, värinä, pakettien katoaminen ja kaiku. (Wallingford 2005, 191.)



CoS:n eli Class of Service on QoS:n käsite, jonka taustat ovat perinteisessä puhelinverkkojärjestelmässä. CoS on kokoelma protokollia, joka toimii OSI-mallin datalinkkikerroksella. CoS priorisoi liikennettä yksittäisissä datalinkeissä ja yksittäisten hyppyjen välissä tarkkailemalla verkon liikennettä ja luokittelee sittemmin liikennöitävää dataa eri käyttäytymismallien mukaan. (Wallingford 2005, 196.)

IEEE:n 802.1q-standardi virtuaaliselle lähiverkolle, VLAN:lle (Virtual Local Area Network), mahdollistaa ääni- ja videoliikenteen erottamisen muusta dataliikenteestä. Virtuaalisessa LAN:ssa liikenne kulkee fyysisesti samassa, mutta loogisesti eri lähiverkossa. Tällä tavoin liikenteen priorisointi on helpompaa. (Wallingford 2005, 203.)

Parhaimman tuloksen saamiseksi kannattanee käyttää useampaa lähestymistapaa. Verkko kannattaa virtualisoida kahteen tai useampaan VLAN:iin sekä käyttää yhtäaikaisia protokollia, kuten esimerkiksi otsikkotietojen avulla pakettien välitystä solmujen välillä yksinkertaistavaa MPLS:ä (Multiprotocol Label Switching) sekä resursseja hallinnoivia RSVP:tä ja DiffServiä, jotka arvottavat liikennettä niin, että kriittisin data kulkee ensin. (Wallingford 2005, 198 - 203.)

Kolmibittistä 802.1p-protokollatietoa ja ToS-tietoa eli Type of Serviceä käytetään lähiverkoissa liikenteen priorisoimiseksi. Nämä tiedot IP-pakettien otsikkotiedoissa ilmoittavat liikennöidyn datan tyypin ja arvon. Tällaisia eri tietotyyppisiä ovat esimerkiksi Routine, Priority, Flash, Internet ja Network. (Wallingford 2005, 196.)

DiffServ (Differentiated Services) -protokolla vastaa yleisesti point-to-point WAN-verkkojen CoS:stä. DiffServ käyttää ToS-otsikkotietoja sekä erilaisia policyserveiltä, COPS:ilta (Common Open Policy Server), saamia sääntöjä. Saatujen sääntöjen perusteella liikennettä priorisoidaan verkon reunalla sijaitsevassa reitittimessä. Pakettien otsikkotiedoissa voidaan myös määrittää sen tärkeys DSCP (DiffServ Code Points) -luokittelulla. Esimerkkinä DCSP-luokista ovat BE eli Best Effort sekä AF eli Assured Forwarding. Point-to-point-yhteydet

ovat yleensä hyvin leveäkaistaisia, jolloin muita sääntelytekniikoita ei yleensä tarvita. (Wallingford 2005, 198.)

## 2.5 VoIP-järjestelmän tietoturvasta ja tietoturvaratkaisuista

VoIP-järjestelmän liikenne kulkee IP-verkossa, jolloin VoIP:ssa on myös samat riskit kuin tavallisessa IP-pohjaisessa liikennöinnissä. Perinteisessä puhelinverkkoympäristössä, jossa jokaiselle yhteydelle on varattu oma kuparilinjansa, on puheluiden salakuuntelu ja häirintä on työläämpää. (Plewes 2007.)

Yleisimpiä vaaroja, joihin tulee osata varautua IP -verkossa liikennöitäessä, ovat DoS (Denial of Service)-, Buffer Overflow- ja man-in-the-middle-hyökkäykset, spämmäys, tietojen kalastelu, hakkerointi sekä liikenteen salakuuntelu. VoIP:ssa käytetty selkokielineen SIP (Session Initiation Protocol) tuo myös mukanaan omat riskinsä. (Plewes 2007.)

Käyttämällä ajan tasalla olevia antivirus-ohjelmia, palomureja ja valvomalla sekä rajoittamalla liikennettä verkkoon ja verkosta poispäin voidaan estää tunkeilijoita pääsemästä käsiksi verkkoon ja sen tietoihin. Verkkoinfrastruktuurin pitää olla riittävän vikasietoinen ja riisuttu ylimääräisistä ominaisuuksista. (Plewes 2007.)

VoIP-järjestelmissä spämmäys ei ole vielä yleistä, mutta siihenkin tulee varautua. Perinteiset sisällönsuodattimet eivät VoIP:n tapauksessa käy, mutta vastaavaa äänitunnisteita vertailevaa suojaa ollaan kehittämässä. NEC Corporationin kehittämä VoIP Seal saattaa olla yksi ratkaisu SPIT (Spam over Internet Technology) -ongelmiin. (Plewes 2007.)

Phissing eli käyttäjä tietojen, salasanojen ja luottokorttinumeroiden urkinta on käyttäjien tietämättömyyteen ja asiasta tiedottamiseen liittyvä vaara, jota kutsutaan myös termillä social engineering. VoIP-järjestelmissä samaa asiaa ajaa vishing eli voice phissing. Vishingin idea pohjaa soittajien ID-tunnisteiden spoofaamiseen ja ihmisten ylenpalttiseen luottamukseen soittajan todellisesta identiteetistä. Ratkaisuksi tarjotaan yleistä asenteiden muuttamista sekä parempaa tiedottamista tietoturvariskeistä käyttäjille. (Plewes 2007.)

Lisäturvaa verkkoon saadaan esimerkiksi kryptaamalla lähetettyä dataa sekä todentamalla ja autentikoimalla käyttäjiä. Lisäksi voidaan ottaa verkossa käyttöön access control eli erilaisiin policyihin perustuva pääsynvalvonta. Lisäturvaa saadaan myös analysoimalla verkon liikennettä IDS:eillä (Intrusion Detection System), tunkeilijan havaitsemisjärjestelmillä. (Wallingford 2005, 224 - 226).

## 2.6 VoIP-tekniikan tuomat palvelut yrityksille

Yrityksille VoIP tuo keskitetysti hallittavan puhelujärjestelmän, joka tarjoaa lisää työkaluja kommunikointiin. VoIP toimii tehokkaasti erilaisten verkkosovellusten kanssa sekä vähentää puheluliikenteen kustannuksia. VoIP-järjestelmien avulla voidaan tallentaa, etsiä ja kerätä yhteen tietoja puheluista ja käyttäjistä, mikä helpottaa myös puhelujen määrien seuranta ja niiden laskutusta. (VoIP 2009.)

VoIP mahdollistaa suuren määrän eri toimintoja ja ominaisuuksia, jotka tuovat joustavuutta työmaailmaan. Lista on pitkä, mutta yksiä monista ovat ryhmä- ja push-to-talk-puhelut, puhelu- ja soittoryhmät, soittajan tunnistaminen, puhelinluettelot, puhelunsiirto ja -välitys, puhelutietojen seuranta ja niiden tallentaminen sekä sisä- ja konferenssipuhelut. Yksi olennainen ominaisuus VoIP:ssa on se, ettei puhelimen käyttämä numero ole enää riippuvainen siitä, missä puhelin on kiinni, vaan puhelinta voidaan liikutella ja käyttää missä päin verkkoa tahansa. (Wallingford 2005, 94 - 109.)

Verkon ylläpitäjää miellyttäviä ominaisuuksia ovat perinteistä puhelinverkkoa huomattavasti yksinkertaisempi ja helppokäyttöisempi, keskitetty hallintarajapinta sekä verkon nopea toipuminen ongelmatilanteissa. Mikäli yksi reitti on poikki, reitittää järjestelmä puhelun automaattisesti toista reittiä. Puhelutietoja voidaan myös logittaa. Logitietojen avulla saadaan kerättyä tietoa verkon kapasiteetista sekä käytöstä ja näiden pohjalta ryhtyä tarvittaessa muuttamaan verkon resursseja. (Wallingford 2005, 97.)

### 3 VOIP:N SIGNALOINTIPROTOKOLLAT

Signaalointiprotokollien tarkoituksena on signaloida ja tallentaa siirrettävää mediaa. Samaiset protokollat myös avustavat järjestelmää puhelujen aloituksessa ja lopetuksessa sekä silloin, kun VoIP-järjestelmää käytetään tiedonsiirtoon tai usean osapuolen välisiin videopuheluihin. (Wallingford 2005, 130.)

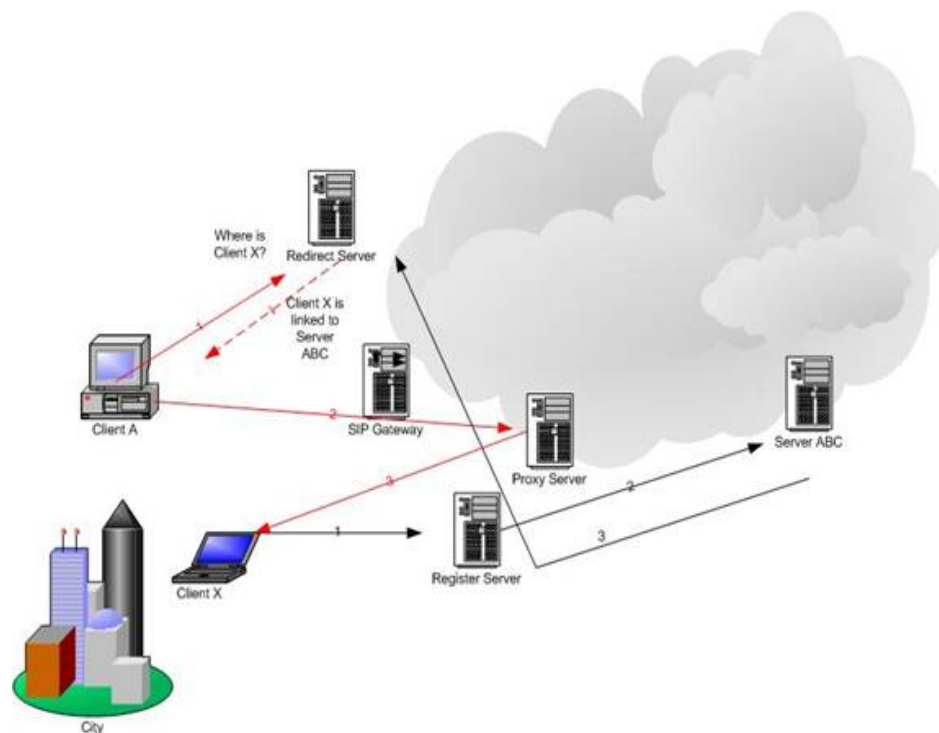
Puhelusignaali lähetetään VoIP:ssa UDP:nä, mutta sitä ei silti nähdä verkossa reaaliaikaisena liikenteenä. Signaloinnista lähetettävä tieto liikennöidään lyhyinä ja purskeisina viesteinä. SIP ja H.323 ovat käyttäjän puolisen pään protokollia, joita verkon ylläpitäjät hallinnoivat. Muut signaalointiprotokollat ovat yleisimmin operaattoreiden ja palveluntarjoajien käytössä. (Wallingford 2005, 130.)

#### 3.1 SIP - Session Initiation Protocol

SIP on IETF:n kehittämä sovelluskerroksen protokolla, joka on omanlaisensa ajattelumalli verkossa käytävien mediaistuntojen suorittamiseksi. SIP:ssa verkon laitteita kutsutaan nodeiksi, jotka liikennöivät keskenään HTTP:n kaltaisin viestein. SIP:ssa käytettyjä viestejä ovat muun muassa INVITE, ACK, BYE, CANCEL, REGISTER ja NOTIFY. Protokollaa käytetään paikantamaan

istuntojen osapuolet verkossa sekä luomaan, ylläpitämään ja päättämään käydyt multimediaistunnot. (Wallingford 2005, 149 - 151.)

SIP-verkko koostuu UA:eista (User Agent) ja SIP-servereistä (KUVIO 2). SIP-servereitä on kolme eri tyyppiä. Registrar toimii käyttäjien rekisteröintiserverinä ja ylläpitää käyttäjien paikkatietoja. SIP-proxy ja redirect-serverit ohjaavat puheluja edelleen verkossa, istuntojen otsikkotietojen perusteella. User Agentit voidaan jakaa kahteen alakategoriaan: UAC:eihin (User Agent Client) ja UAS:eihin (User Agent Server). UAC:t lähettävät pyyntöjä, joilla istuntoja muodostetaan ja muokataan ja joihin UAS:t generoivat sittemmin vastauksia ja ryhtyvät tarvittaviin toimenpiteisiin istuntoja luodakseen. (Rosenberg & Schultsrinne 2002.)

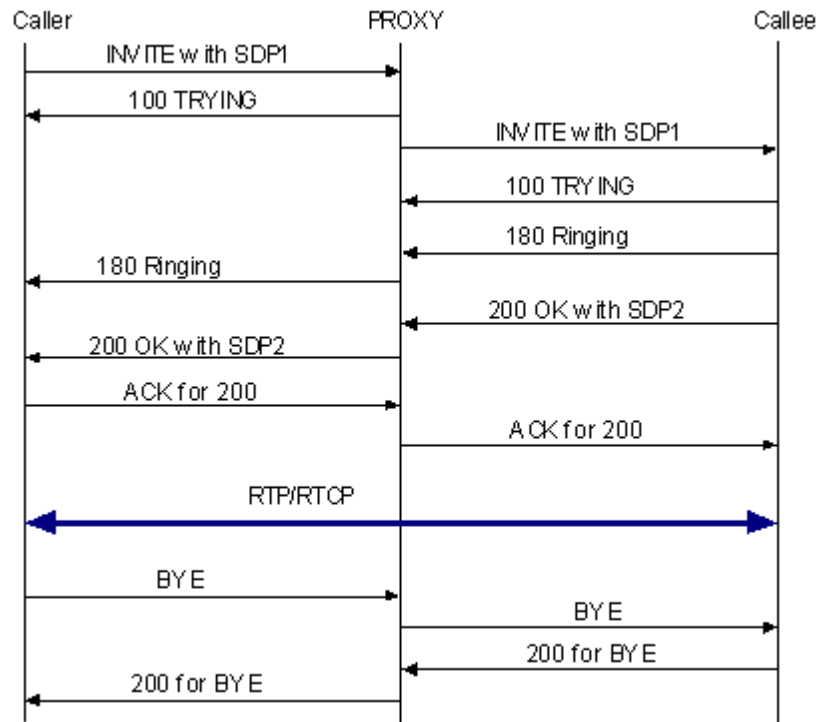


KUVIO 2. SIP-arkkitehtuuri (Magalhaes 2005)

### 3.1.1 SIP-istunto

SIP-multimediaistuntoa luodessa käydään useita keskusteluja laitteiden välillä. Tällaisia keskusteluja ovat käyttäjien paikannus verkossa, vastaanottajan saavutettavuus, istunnon aikana käytetyn median ja sen parametrien määrittely, istunnon luonti sekä istunnon hallinta. Jokaiselle käyttäjälle määritellään yksilöllinen SIP URI (Uniform Resource Identifier), jota käytetään yksilöivänä osoitetietona verkossa. URI on yleensä muotoa käyttäjätunnus @ domainin host-nimi, esimerkiksi sip:sipella@siphost.com. (Rosenberg 2002.)

Liikennöinti aloitetaan sopimalla ensin osapuolien välille avattavan istunnon määrittelyt SDP:llä (Session Description Protocol). SIP-puhelun kulku käydään metodeilla (KUVIO 3) ja itse mediaistunto liikennöidään RTP:llä (Real-time Transport Protocol) ja RTCP:llä (Real-time Control Protocol), jotka määrittelevät, miten lähetettävä media paketoidaan sekä miten voidaan varmistua istunnon QoS-toiminnasta. Käyttäjien autentikointi istuntoa varten SIP-sovelluksissa suoritetaan yksipuolisella autentikoinnilla, palvelimelta käyttäjän suuntaan, käyttäen esimerkiksi salaavaa TLS-prokollaa (Transport Layer Security). (Wallingford 2005, 155.)



KUVIO 3. SIP-puhelun liikennöinti (Packetizer 2009)

SIP perustuu tiedon vaihtoon yksittäisten kyselyjen ja näiden vastausten avulla. Jokainen kysely herättää jonkin metodin tai toiminnon serverin päässä tai serveri virhetilanteen sattuessa vastaa kyselyyn tiedoksiantavalla vastauksella siitä, mikä meni vikaan. (Rosenberg 2002.)

Istunto aloitetaan lähettämällä INVITE-viesti halutulle vastaanottajalle/ vastaanottajille osoitetietona vastaanottajan URI-osoite. INVITE-viestin header-tiedoissa kulkee istuntoa koskevia SDP-tietoja, joiden mukaan määritellään istunnon parametrit yhteneväisiksi kaikille osapuolille. Header-kentässä kulkee myös istunnon tyyppitiedot sekä lähettävän osapuolen URI-osoite. (Rosenberg 2002.)

INVITE-viesti kulkee SIP-proxyjen kautta vastaanottajalle, joka halutessaan vastaanottaa mediaistunnon vastaa OK-viestillä, jonka lähettävä osapuoli vahvistaa ACK-viestillä. Kolmisuuntaisen kättelyn jälkeen RTP:llä liikennöity

mediaistunto aukeaa ja se käydään suoraan osapuolten välillä. Kun istunto halutaan päättää, lähetetään BYE-viesti proxyn kautta yhteydenottajalle, jonka tämä vahvistaa saaduksi OK-viestillä ja SIP-istunto sulkeutuu.

(Rosenberg 2002.)

### 3.1.2 SIP ja NAT

Liikennöitäessä sisäverkosta ulkoverkkoon NAT (Network Address Translation) on useasti käytetty toiminnallisuus yrityksen verkossa. NAT piilottaa lähettäjän sisäverkossa käytetyn IP-osoitteen (KUVIO 4) ja käyttää määrättyä julkista IP-osoitetta liikennöimään vastaanottajalle ulkoverkkoon. NAT:n avulla voidaan vähentää käytettyjen julkisten osoitteiden määrää. Liikennöitäessä SIP:llä ulkoverkkoon aiheuttaa NAT:n käyttö verkon reunalla ongelmia eritoten silloin, kun halutaan liikennöidä ulkoverkon läpi omaan loogiseen lähiverkkoon.

(Cisco Systems 2007.)

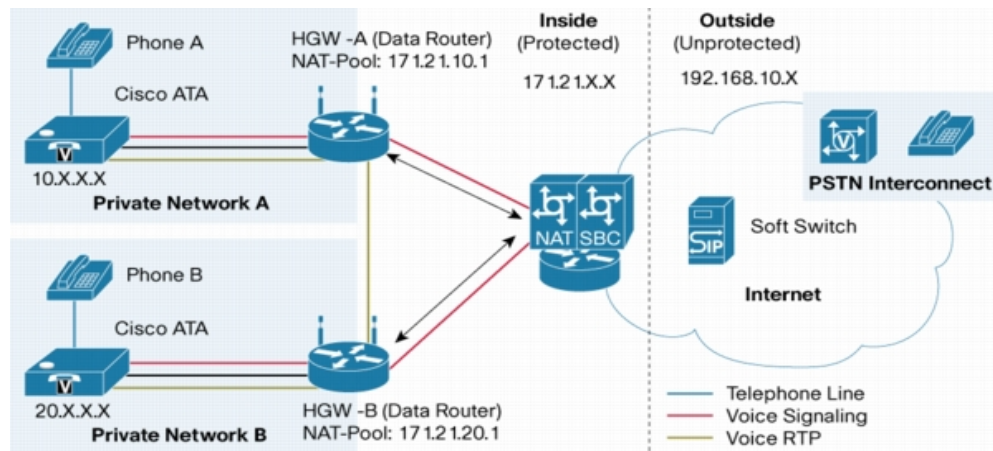
Tilanne ei ole kuitenkaan mahdoton. Yksi ratkaisu SIP liikenteen toimittamiseen sujuvasti NAT:n läpi on STUN (Simple Traversal of UDP Through Network Address Translation). Cisco Systems on ollut mukana kehittelemässä kyseistä protokollaa, joten yhteensopivuus Ciscon laitteiden kanssa lienee taattu.

Käytännössä STUN toimii niin, että se kertoo ulospäin liikennöivälle STUN-clientille tämän käyttämän julkisen IP-osoitteen ja määrätyn portin, jonka kautta liikenne sittemmin kuljetetaan. Ongelmaksi kuitenkin jäävät verkon ulkopuolelta NAT:lle saapuvat TCP-paketit. (Cisco Systems 2007.)

Cisco Systems tarjoaa laitteilleen NAT tuen SIP-toiminnoille yrityksen verkkoympäristöissä. Tämä Connection-Oriented Media Enhancements (Comedia) for SIP-ominaisuus mahdollistaa symmetrisen NAT-traversal menetelmän käytön. Comedia sallii Ciscon gatewayn tarkistaa tulevien RTP-pakettien lähettäjän sekä sallii päätepisteiden mainostaa itseään, olivatpa ne NAT:n sisä- tai ulkopuolella. Rajoitteena tälle ominaisuudelle on, että käytettävissä ovat vain IPv4-osoitteet. Symmetrisessä NAT:ssa kaikki pyynnöt



verkon sisäpuoliselta IP-osoitteelta ja portilta ohjataan määriteltyyn ulkoiseen IP-osoitteeseen ja porttiin. (Cisco Systems 2007.)



KUVIO 4. NAT ja SIP (Cisco Systems 2009)

### 3.2 H.323

ITU:n kehittämä, H.323-standardi antaa määrittelyt PBX (Private Branch Exchange) -tyyliseen, yrityksen sisäisen puhelinjärjestelmän signaalointiin. Toisin kuin SIP:ssä, H.323:n kättelyviestit ovat lyhyitä ja kompakteja, jolloin myös liikennöinti on nopeaa. Ajatuksena H.323:ssa on siirtää mahdollisimman vähän signaalointidataa ja mahdollisimman paljon multimediaa.

(Wallingford 2005, 134.)

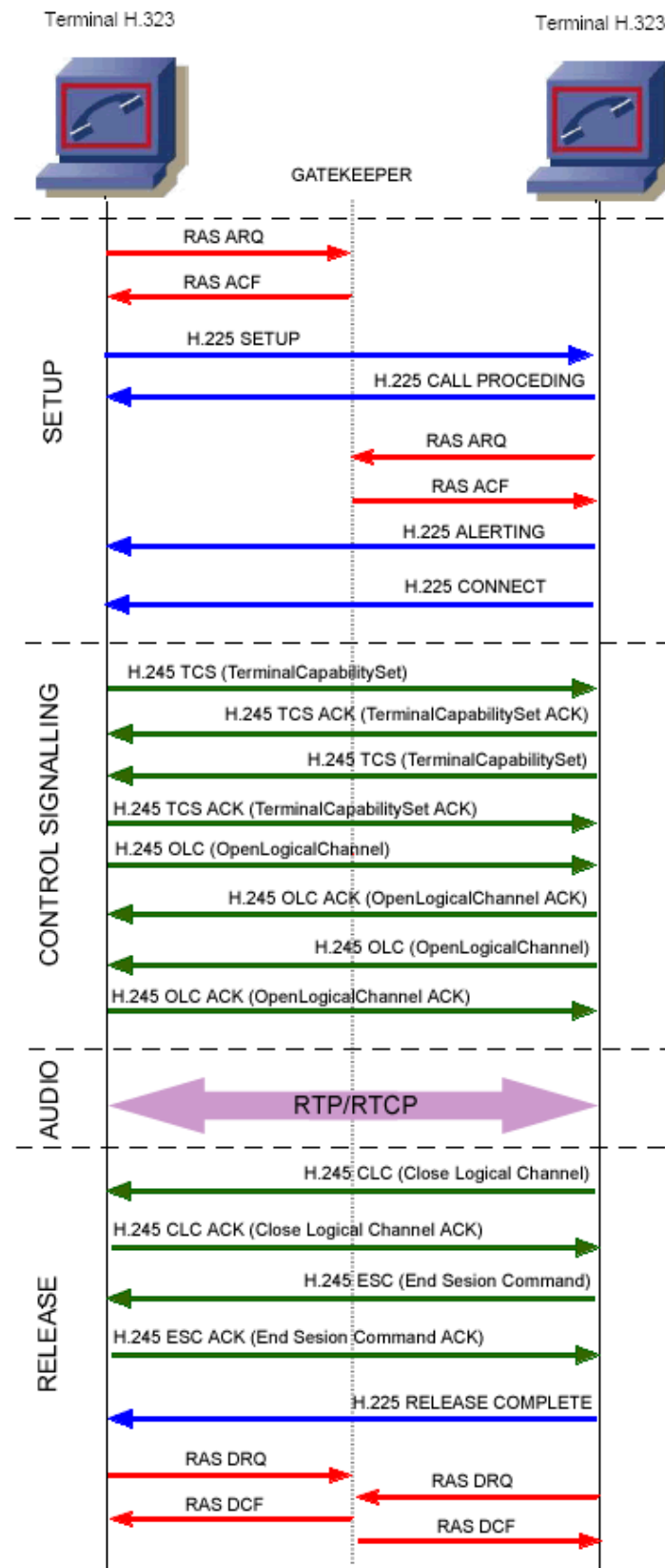
H.323 on eräänlainen sateenvarjoprotokolla, joka määrittelee monen osallistujan välisen VoIP-ympäristökokonaisuuden ja jonka alaprotokollat määrittelevät sittemmin itse mediaistunnon ja sen toiminnot. Nämä alemmantason protokollat ovat H.245, H.225 ja Q.931. H.245 protokolla kontrolloi kanavan resursseja sekä datan signaalointia. H.225 vastaa myös signaloinnista ja sen lisäksi käyttäjien rekisteritiedoista eli RAS:ista (Registration Admission Status). Q.931 on taas

määrittäminen ISDN-puhelujen toteuttamiselle. Lisäksi H.323:n alta löytyy useita määrittämiä eri kodekeille sekä liityntärajapinnoille. (H.323 Standards 2002.)

### 3.2.1 H.323-istunto

H.323 Gatekeeper (KUVIO 5) toimii päätelaitteiden eli terminaalien välillä seuraten keskitetysti liikennettä sekä signalointiresursseja. Gatekeeper tarjoaa myös E.164 (ITU:n määrittäminen kansallisille ja kansainvälisille puhelinnumeroille) -standardin mukaisen osoitteiden selvityksen, käyttäjien sekä puhelujen autentikoinnin ja käytettävän median resurssien hallinnan. (Wallingford 2005, 135.)

Jokaisen terminaalin tulee rekisteröityä Gatekeeperille RAS (Registration, Authentication and Status) -protokollaprosessin mukaisesti. H.225 protokollan viesteillä hoidetaan istunnon aloittaminen, ylläpito ja päättäminen, kun taas H.245-protokolla hoitaa loogisen istunnon aukaisemisen ja sulkemisen, sopii käytettävän RTP-profiilin, ikkunakoon, käytetyn kodekin sekä neuvottelee siirrettävän median tyyppiä. RTP- ja RTCP-protokollat huolehtivat äänen, videon ja instant messaging-palvelujen datastreamien siirrosta sekä niiden QoS:sta. (Wallingford 2005, 137 - 141.)



KUVIO 5. H.323-istunto (Voipforo 2007)

### 3.2.2 H.323:n tunnelointi NAT:n läpi

Liikennöitäessä dataa H.323-protokollaa käyttäen osoittautuu NAT ongelmaksi, sillä lähettäjän ja vastaanottajan osoitetiedot on määritelty H.323:ssa myös H.323-paketin sisälle, paketin payload-tietoihin. NAT:n läpi siirryttäessä ulommat TCP/IP-header tietoihin kirjatut osoitetiedot muuttuvat ja H.323-paketin sisemmät osoitetiedot ovat tällöin ristiriidassa ulompien osoitetietojen kanssa. Eri osoitetiedot tuottavat vastaanottajan päässä hämmennystä. H.323:n ja NAT:n yhteistoiminnassa ilmenevä ongelma voidaan korvata käyttämällä H.323-tietoisia reitittäjiä, jotka osaavat tarvittaessa kaivaa osoitetietoja myös syvemmmältä. Tällaiset laitteet kuitenkin rajoittavat muuten koko verkkoinfran rakentamista, sillä ne ovat yleensä hyvin valmistajakohtaisia eikä yhteensopivuutta voida taata. (Tittel 2001.)

Toinen vaihtoehto on käyttää tunnelointitekniikkaa kuljettamaan H.323 NAT:n lävitse haluttuihin verkkoihin tai NAT:n takana oleviin omiin aliverkkoihin. H.323-istunnot NAT:n yli voidaan siis toteuttaa eri portteihin määriteltyjen VPN (Virtual Private Network) -tunnelien avulla. (Tittel 2001.)

### 3.3 Muita signalointiprotokollia

MGCP ja H.248, eli Megaco, ovat operaattorien ja VoIP-palveluntarjoajien käyttämiä signalointiprotokollia, jotka määrittelevät signalointitoimintoja useiden Media gatewayden välille. Nämä kaksi protokollaa määrittelevät myös sen, kuinka perinteisestä puhelinverkosta voidaan liikennöidä IP-pohjaiseen verkkoon. (Wallingford 2005, 158 - 159.)

Ciscon Systemssin kehittämä Skinny Client Control on protokolla VoIP-järjestelmien signalointiin. SCCP on lähinnä tarkoitettu käytettäväksi Ciscon omien tuotteiden, Call Managerin ja Ciscon IP-puhelimien kanssa. SCCP määrittelee clienttien ja Call Managerin väliset istunnot, niiden avaamisen ja sulkemisen. Multimedialiikenne kulkee RTP-mediastreaminä, niin kuin muillakin standardeilla. SCCP:tä harvemmin käytetään sellaisenaan ja sitä yleensä sovelletaankin H.323-protokollan kanssa. (Wallingford 2005, 160.)

## 4 KOHTI LANGATONTA JÄRJESTELMÄÄ

Siirtyminen kiinteästä VoIP:sta, ainakin osittaiseen langattomuuteen, on nykypäivänä normaali kehityssuunta. Mobiilius on hyvin tärkeää nykypäivän yritysmaailmassa. Liikkuvuus tuo tehokkuutta ja tehokkuus rahallisia säästöjä. (Cisco Systems 2008.)

Langattomalle VoIP:lle on useita nimityksiä, Voice over wireless LAN eli Vo-WLAN, Vo-Fi, VoWi-Fi, wireless VoIP tai VWLAN. Kaikki edellä mainitut ovat siis käsitteitä, jotka voidaan mieltää termiksi, joka tarkoittaa multimediajärjestelmää, jossa dataa siirretään IP-pohjaisessa verkossa langattomasti. VoWLAN ei teknisesti niinkään eroa kiinteästä VoIP:sta, mutta kun siirtotie muuttuu kaapelista ilmatieksi, tuo se mukanaan uusia vaatimuksia koko järjestelmälle. Näitä vaatimuksia tukemaan on otettava kourallinen langattoman verkon 802.11-standardien lisämäärittelyjä, joista tärkeimpiä ovat verkkoliikenteen QoS:sta huolehtiva 802.11e- ja tietoturvasta vastaava 802.11i-standardi. (Cisco Systems 2008.)

### 4.1 VoIP ja langaton siirtotie

IEEE:n 802.11-standardin mukaisessa langattomassa verkossa voidaan liikennöidä IP-pakettidataa, ja standardin mukainen verkko toimii näin ollen myös siirtotienä VoIP-järjestelmän liikenteelle. 802.11-työryhmä on määritellyt neljä langatonta nopeusluokkaa, 802.11a, 802.11b, 802.11g ja 802.11n, joista b, g ja n toimivat 2,4 GHz:n ja a ja n 5 GHz:n taajuuksilla. (Hintikka 2004.)

Nykyään langattomien verkkojen todelliset tiedonsiirtonopeudet voivat nousta 100:sta - 200 Mbit/s:ssa ja teoreettisten nopeuksien sanotaan nousevan jopa 600 Mbit/s:ssa. 802.11-työryhmä on laatinut lisäksi useita laajennuksia verkon laadun, tietoturvan ja verkkojen välisten siirtymisten tueksi. Alun perin 802.11-standardia ei suunniteltu lainkaan kuljettamaan ääntä, mutta erilaisilla lisäasetuksilla saadaan se kuitenkin onnistumaan. (Hintikka 2004.)

#### 4.1.1 Liikenteen priorisointi

Langattomassa VoIP-järjestelmässä voidaan käyttää langattomalla verkkokortilla varustettuja matkapuhelimia, dual-mode-puhelimia, joissa erillinen client-ohjelma ottaa yhteyden VoIP-puhelukeskukseen. Cisco Systemsin laitteita käyttävälle yritykselle tämä keskus on Call Manager-ohjelmarajapinta, jolla hallinnoidaan soittajia ja näiden tietoja. Ilman mitään lisävarusteluja matkapuhelimet eivät osaa kuitenkaan kuunnella toistensa sijaintia ja lähetyksiä, jolloin ongelmia saattaa syntyä. (Phifer 2005.)

Yksi vaihtoehto, jolla voidaan parantaa lähetystehokkuutta ja toisaalta vähentää törmäyksiä, on jakaa data- ja ääniliikenne omiin verkkoinfrastruktuureihinsa. Toinen, halvempi vaihtoehto, on jakaa verkko erillisiin virtuaaliverkkoihin, dataliikenne ja ääniliikenne omiin VLAN:eihinsa. (Phifer 2005.)

Langattomassa liikenteessä käytetään CSMA / CA (Sense Multiple Access with Collision Avoidance) -kaistanvarausmenetelmään pohjaavaa DCF- mekanismia (Distributed Coordination Function) avustamaan langattomalle siirtokaistalle pääsyn hallintaa. CSMA / CA:ssa lähettävät osapuolet kuuntelevat siirtomediaa, ja mikäli kukaan muu ei siellä liikennöi, voivat he lähettää dataa siirtotielle. Jos kaistalla tapahtuu törmäys, lähetys lopetetaan ja kaikki osapuolet pitävät satunnaisen pituisen tauon, jonka jälkeen voidaan taas yrittää käyttää kaistaa. Reaaliaikaiselle datasiirrolle tällainen ei riitä, vaan tarvitaan varmuus siitä, että

liikenne sujuu sulavasti eivätkä virheet lähetyksissä haittaa sovellusten toimimista. (Phifer 2005.)

802.11e määrittelee kilpavaraukseen perustuvan menetelmän, EDCA:n (Enhanced Distributed Channel Access), jossa pakettiliikenne voidaan jakaa eri arvoluokkiin, video-, voice-, best-effort- ja background-tageilla, ja joiden perusteella priorisointi sittemmin suoritetaan. Kehyksiä voidaan pilkkoa myös pienemmiksi, mikäli ne ylittävät EDCA:lle määritelly aikavälin, transmission opportunityn, TXOP:n. Luokittelemalla lähetettävää liikennettä parannetaan liikennöinnin varmuutta ja sujuvuutta. (Phifer 2005.)

#### 4.1.2 802.11e – QoS-määritykset langattomalle verkolle

802.11e on IEEE:n määritys Quality of Servicelle langattomassa verkossa.

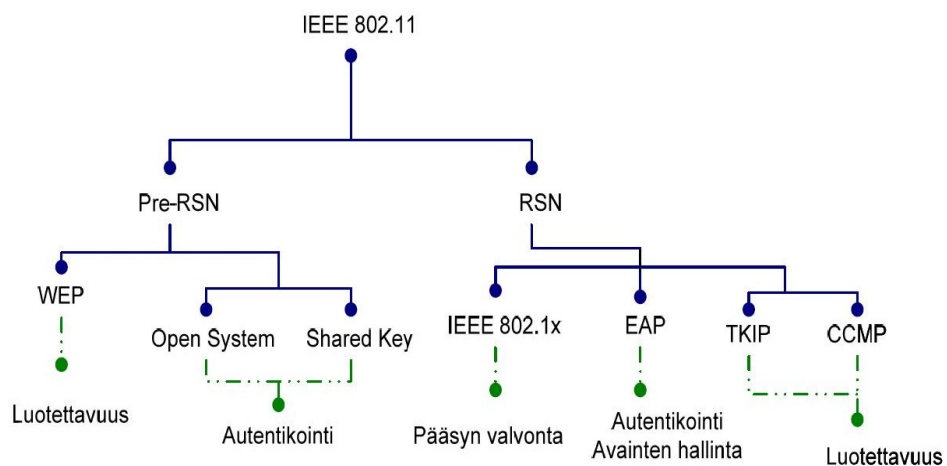
802.11e priorisoi langatonta pakettiliikennettä MAC-tasolla, sille annettujen arvoluokitusten perusteella. Liikenteen priorisoinnin merkittävyys kasvaa suhteessa langattoman liikenteen määrään. Toisin kuin tavallinen dataliikenne, reaaliaikaiset ääni- ja videosovellukset ovat hyvin herkkiä aikaviiveille ja tarvitsevat nopeaa palvelua, jotta palvelujen toimivuus voidaan taata. (Hintikka 2004.)

IP-pakettiliikenteen priorisoinnin lisäksi QoS-toiminnot huolehtivat siitä, ettei paketteja häviä matkalla eikä liikenteeseen tule viiveitä ja että tukiasemiin tuleva ja niistä lähtevä liikenne liikkuu sulavasti. QoS-komponenttien avulla pyritään vähentämään kanavien ylikuulumista, helpottamaan handoff-prosesseja tukiasemien välillä, ts. siirtymissä solusta toiseen, sekä vähentämään ympäristöstä tulevien radioaaltojen vaikutusta tiedonsiirtoon. (Hintikka 2004.)



#### 4.2 802.11i-standardi ja VoWLAN-järjestelmän tietoturvallisuus määrittelyt

Langattomalle verkolle on luonteenomaista kertoa kaikki itsestään niille, jotka ovat verkon kantoalueella, jolloin on tärkeää, että liikennöitävä data salataan ja verkkoon liikennöivät käyttäjät autentikoidaan. IEEE loi 802.11i-standardin (KUVIO 6) määrittelemään tietoturva-asetuksia langatonta verkkoa käyttäville laitteille. 802.11i perustuu AAA (Authentication, Authorization and Accounting) -periaatteeseen, jossa käyttäjä tunnistetaan, tämän oikeudet määritetään ja tekemisiä tarkkaillaan. (Griffith 2004.)



KUVIO 6. Langattoman tietoturvan kehitys (Taavila 2008)

Salaus voidaan toteuttaa esimerkiksi TKIP-avainnuksella (Temporal Key Integrity Protocol) ja autentikointi RADIUS-palvelimen kautta käyttäen WPA2:n AES (Advanced Encryption Standard) lohkosalausmenetelmää. Koskaan radiotie siirtotienä ei ole murtamaton ja siksi verkon ylläpitäjien tulee kiinnittää sen käyttöön erityistä huomiota. Muita salausmenetelmiä on useita, joista valitaan verkon kannalta sopivin vaihtoehto. Koska kaikki verkko- ja päätelaitteet eivät tue kaikkia salausmenetelmiä, pitää olla valmis kompromisseihin verkon tietoturva määriteltäessä. (Griffith 2004.)

#### 4.2.1 WPA-2 ja sitä edeltäneet tietoturvaprotokollat

802.11i, joka tunnetaan myös WPA-2-määrittämisinä, on IEEE:n 802.11-standardeille luotu tietoturvalisäys. 24. kesäkuuta 2004 ratifioidussa 802.11i:ssä määritellään uudemmat standardit langattoman verkon tietoturvalle. 802.11i:n uudet ominaisuudet korvaavat edellisten tietoturva spesifikaatioiden, WEP:n (Web Equivalent Privacy) ja WPA:n (Wi-Fi Protected Access), heikkoudet. WPA-2 on taaksepäin yhteensopiva, aiemmin määritellyjen WPA:n ja WEP:n kanssa, jolloin myös vanhempien laitteiden tietoturvasovellisuus voidaan edelleen taata. (Savonia ammattikorkeakoulu 2007.)

WEP-salausssä on käytössä vain 64-bittinen, staattinen salausvain. WPA:ssa salausavaimen generointi toteutetaan esimerkiksi TKIP:llä. TKIP:ssä käytetään 128-bittistä pakettikohtaista salausavainta salaamaan lähetetty data ja käytetyt avainparit luodaan dynaamisesti jokaiselle paketille. Molemmat, WEP ja WPA, käyttävät symmetristä jonosalaajaa, RC4:ää. RC4-salausssä olevan puutteen vuoksi joidenkin pakettien kehysissä lähetetään salaamattomia bittejä, alustusvektoreita, ja niiden perusteella voidaan helposti laskea käytetty salausvain. 802.11i:ssä käytetään huomattavasti edeltäjiänsä vahvempaa lohkosalausmenetelmää, AES:a (Advanced Encryption Standard). 802.11i sisältää myös RSN-komponentin (Robust Security Network), AES:iin pohjautuvan CCMP-komponentin (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) sekä 4-vaiheisen kättelymenettelyn. (Savonia ammattikorkeakoulu 2007.)

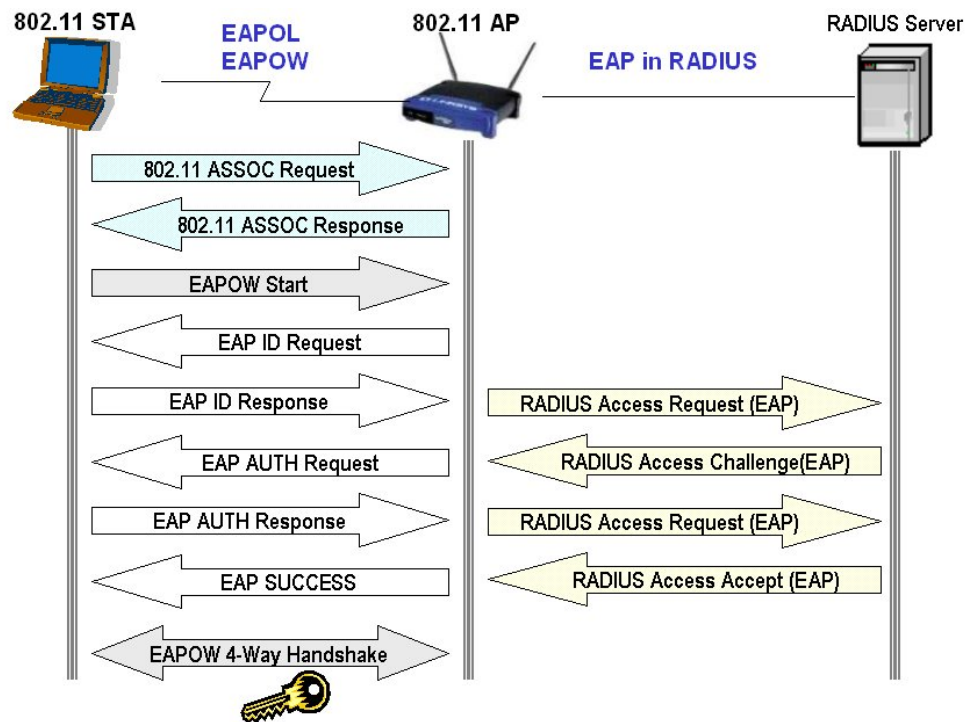
Laillisuustarkastus voidaan langattomassa verkossa toteuttaa monella tavalla. Eräitä laillisuusmenetelmiä ovat PEAP ja LEAP. PEAP on uusi EAP (Extensible Authentication Protocol) IEEE 802.1x-laillisuustarkistustyyppi, joka on suunniteltu tukemaan eri laillisuustarkistusmenetelmiä, mukaan lukien käyttäjän salasanat ja kertakäyttöiset salasanat sekä Generic Token Card-tunnukset. LEAP

on myös EAP (Extensible Authentication Protocol) -yhteydskäytännön versio. LEAP (Light Extensible Authentication Protocol) on Ciscon oma EAP-yhteydskäytäntö, joka antaa käyttöön haaste-vastaus-laillisuustarkistusmekanismin ja avainten dynaamisen määrittämisen. (Savonia ammattikorkeakoulu 2007.)

#### 4.2.2 EAP – protokolla käyttäjien autentikointiin

EAP (Extensible Authentication Protocol) on IEEE:n 802.1x-standardi porttipohjaiselle autentikoinnille LAN- ja MAN-verkoissa. EAP:n avulla toteutetaan verkon reunalla tapahtuva kontrolloitu käyttäjän tunnistus. Autentikoituessa käyttäjä ja AP (Access Point) avaavat yhteyden EAP-kättelyllä (KUVIO 6). EAP-viesteillä todennetaan autentikoituva käyttäjä vertaamalla vastaanotettuja tunnisteita keskitetyssä tietokannassa RADIUS-palvelimella oleviin tunnistetietoihin. Langattomassa verkossa tunnistautuminen tapahtuu vastaavanlaisella EAPOW-menetelmällä (EAP over WLAN). (Puska 2005, 75 - 78.)

Perusajatuksena menetelmässä on luoda käyttäjälle (supplicant) verkkoon kaksi porttia: auktorisoitu ja auktorisoimaton. Käyttäjää tunnistava osapuoli, AP eli verkon liityntäpiste, toimii autentikoijana (authenticator) ja ohjaa auktorisoimattomasta portista vastaanottamansa käyttäjän käyttäjätietojen tiivisteen MD5-tunnistusta (Message Digest 5) ja vie tiivisteen yhteistä salausavainta käyttäen verrattavaksi tunnistuspalvelimelle. Auktorisoimatonta porttia käytetään vain EAP-viestien lähettämiseen. RADIUS-palvelimen tietojen perusteella tehdään päätökset käyttäjän tunnistuksesta ja siitä, siirretäänkö tunnistettava käyttäjä liikennöimään verkkoon auktorisoidun portin kautta. (Snyder 2002.)



KUVIO 6. EAP-kättely (Wi-Fi Planet 2005)

#### 4.3 Handoff-operaatio – joustavuutta mobiiliuuteen

Liikkuvuus on päivän sana. Yksi siihen vaadittava toiminnallisuus on mahdollistaa käyttäjän liikkuminen eri tukiasemien välillä saumattomasti. Päätelaitteen tulee suorittaa handoff-operaatio silloin, kun käytetystä tukiasemasta vastaanotettu signaali alkaa heiketä liiaksi tai kun langattoman verkon kantama loppuu ja laitteen tulee siirtyä lähiverkosta käyttämään toista siirtomediaa. (Lakas & Boulmalf 2005.)

IEEE on määritellyt kaksi standardia, joilla tämän, maksimissaan alle 50 millisekuntia kestävän handoffin, voi toteuttaa. Handoffilla pyritään saumattomaan siirtymään solusta toiseen, eli verkosta toiseen, tai tukiasemalta

toiselle, ilman että puhelun aikana tulee katkoksia, puhelun laatu heikkenee tai että yhteys katkeaa. (Lakas & Boulmalf 2005.)

#### 4.3.1 Langattomien tukiasemien väliset handoff-operaatiot

IEEE julkaisi kesällä 2008, Fast Basic Service Set Transition-tekniikkanakin tunnetun, 802.11r-2008-standardin määrittelemään tukiasemien välistä kommunikointia. Tämä langaton lisästandardi mahdollistaa käyttäjien liikkumisen solualueelta toiselle, esimerkiksi kun käyttäjä liikkuu toimistorakennuksessa eri tukiasemien kantoalueilla ja puhuu samalla aikaa puhelua matkapuhelimellaan käyttäen langatonta, IP-pohjaista siirtomediaa. 802.11r edesauttaa myös verkon suunnittelijaa, sillä standardi poistaa aiemman yhteensopivuusongelman eri valmistajien tukiasemien väliltä. (Goldman 2008.)

Tukiasemien välillä handoff voi olla kahdenlainen, joko make-before-break tai break-before-make. Ensin mainitussa uusi yhteys muodostetaan, ennen kuin vanha katkaistaan. Päinvastaisessa tapauksessa liikennöijä jää hetkeksi ilman yhteyttä mihinkään tukiasemaan, mikä saattaa aiheuttaa häiriöitä äänenlaadussa tai yhteydessä. Kun molemmat tukiasemat, joiden kanssa handoffia hakeva päätelaite keskustelee, ovat saman aliverkon sisällä, voidaan yhteyttä jatkaa toisella tukiasemalla samalla IP-osoitteella kuin aiemmassa tukiasemassa.

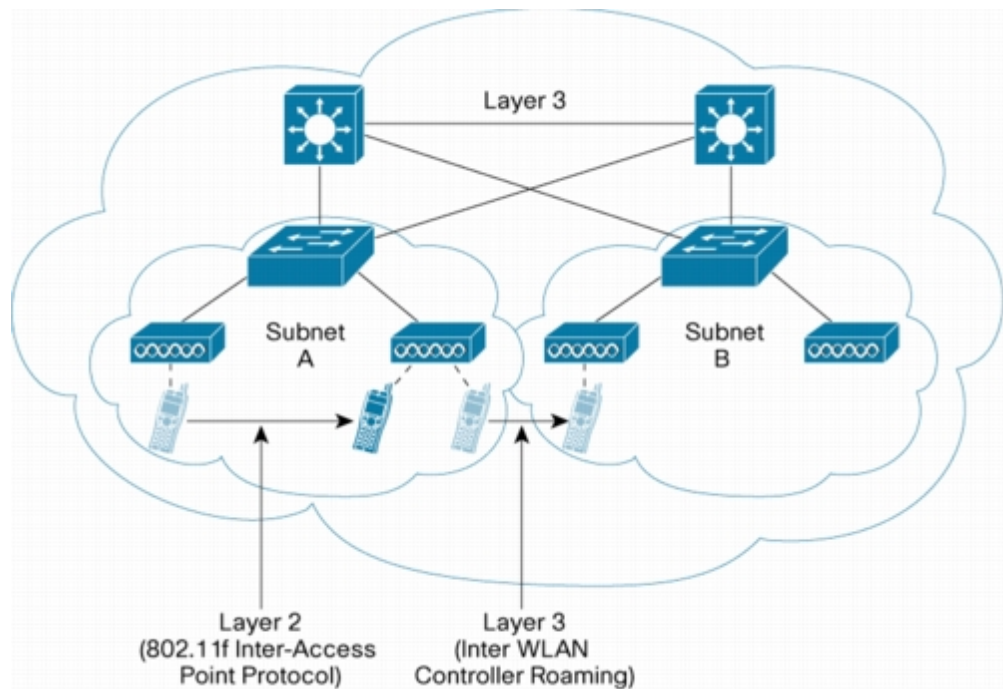
IP-osoitteen säilyminen vauhdittaa handoffia ja vaihtoa voidaan pitää varmempana. (Lakas & Boulmalf 2005.)

Handoff -prosessi lähtee käyntiin, mikäli päätelaite siirtotien signaalia tarkkaillessaan huomaa, että S/N-suhde heikkenee solulle määritellyn lähetystehon alarajalle. Jos näin tapahtuu, alkaa päätelaite paikallistaa alueella olevia muita tukiasemia. (Lakas & Boulmalf 2005.)

Hakuvaiheen alussa (KUVIO 7) kaikki liikennöinti pysäytetään hetkeksi, päätelaite skannaa kantoalueella olevat tukiasemat ja valitsee sopivimman. Kun

vaatimukset täyttävä tukiasema on löydetty, siirretään liikenne kulkemaan uuden tukiaseman kautta ja pudotetaan vanha yhteys pois. Jossain tapauksissa päätelaitteen tulee autentikoitua ja lähettää QoS-profiilinsa määrittämiä tukiasemalle ennen kuin handoff voidaan suorittaa.

(Lakas & Boulmalf 2005.)



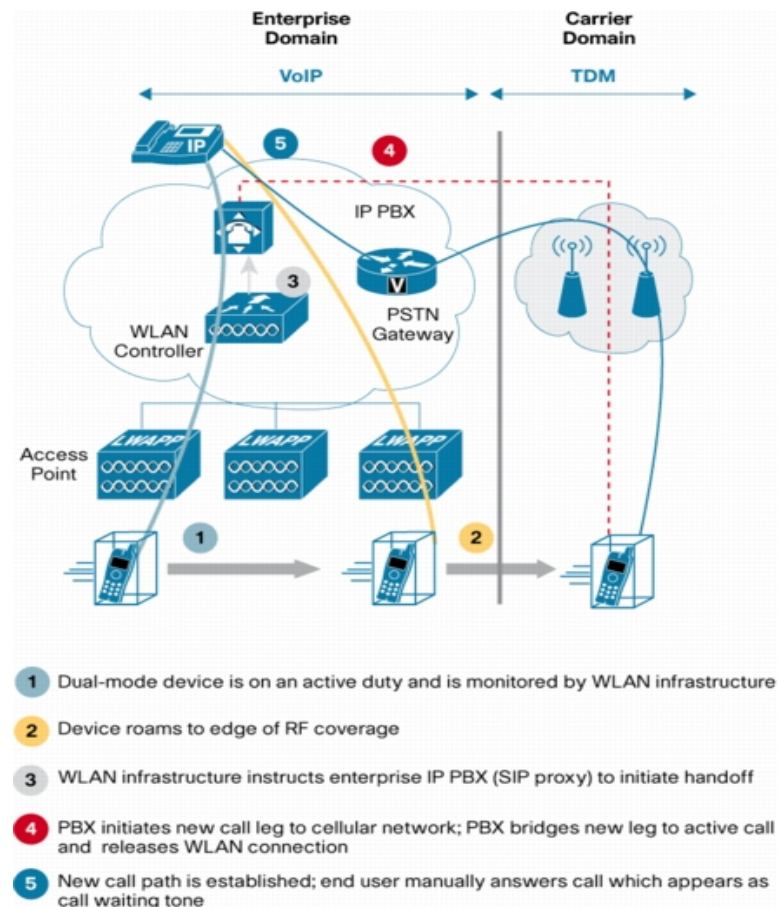
KUVIO 7. Handoff tukiasemalta toiselle (Cisco Systems 2007)

#### 4.3.2 Siirtyminen WLAN:sta GSM-verkkoon

IEEE:n langaton lisästandardiehdotus 802.11u eli WIEN (Wireless InterWorking with External Networks) määrittelee handoffin muihin ulkoisiin verkkoihin (KUVIO 8), kuten matkapuhelinverkkoon. Tämä standardi mahdollistaa siirtymisen puhelun aikana langattoman tukiaseman kantaman päättyessä

liikennöimään häiriöttä matkapuhelinverkkoon. Tämän standardin lopullinen ratifiointi valmistunee vuoden 2010 kesällä. (Wierenga 2009.)

Enterprise WLAN Infrastructure-Controlled Seamless Roaming Based on RSSI (Received Signal Strength Indication) on metodi, jossa puhelujen handoffin langattomasta sisäverkosta mobiiliverkkoon hoitaa yrityksen IP-PBX eli VoIP-puhelinjärjestelmä. Tällöin VoIP-puhelimen ollessa yrityksen WLAN-verkon kantoalueella puheluliikenne ohjataan yrityksen sisäisen VoIP-järjestelmän kautta. Käyttäjän liikkuessa yrityksen langattoman verkon kantoalueen ulkopuolelle suoritetaan handoff matkapuhelinjärjestelmään. Yrityksen WLAN-infrastruktuuri monitoroi aktiivisesti päätelaitteita ja näiden vastaanottamaa signaalitaso ja suorittaa sittemmin tarvittavia toimenpiteitä. (Cisco Systems 2007.)



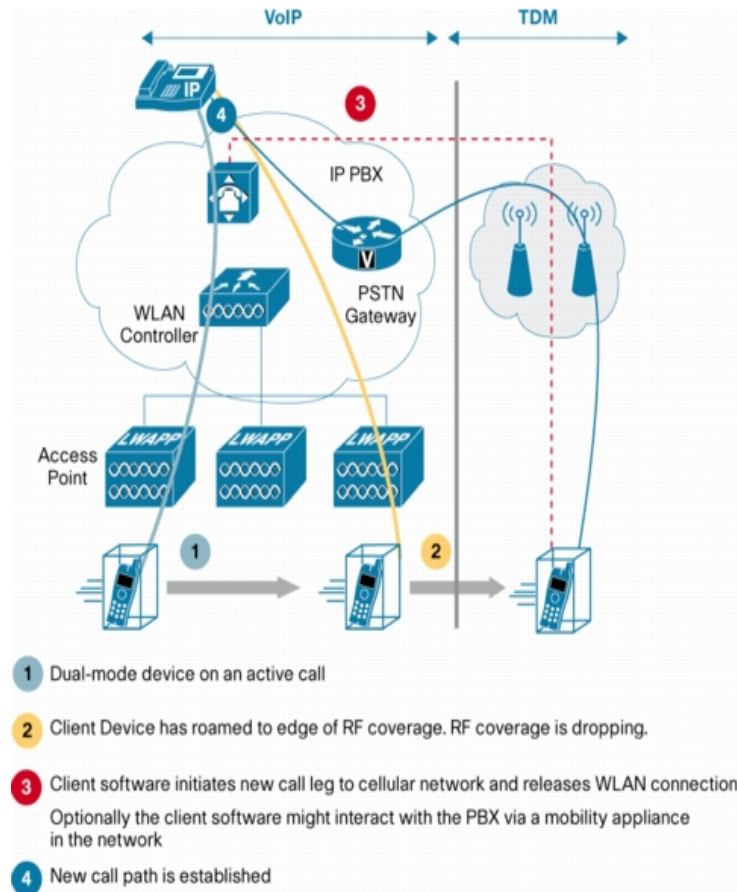
KUVIO 8. WLAN-infran toimintaan keskittyvä handoff (Cisco Systems 2007)

Tällaisen järjestelmän eduksi luettava ominaisuus on, että dual-mode päätelaitteilta ei vaadita muuta kuin toiminnallisuutta tukeva client-ohjelmisto. Ongelmia esiintyy kuitenkin silloin, jos puheluitunto kulkee VPN:n tunnelin lävitse. Myös eri valmistajien välisten laitteiden yhteensopivuus saattaa aiheuttaa ongelmia handoff-toiminnallisuudessa. (Cisco Systems 2007.)

Toinen menetelmä, jolla handoff-prosessi langattoman- ja matkapuhelinverkon välillä voidaan toteuttaa, on nimeltään ”Enterprise Mobile Client-Controlled Seamless Roaming Based on RSSI”. Tässä vaihtoehdossa WLAN-verkkoinfran osallistuminen handoff-tapahtumaan on riisuttu minimiin ja dual-mode laitteen client-ohjelmisto on toiminnan vastuunkantajana. Client tarkkailee aktiivisesti vastaanottamaansa signaalitasoa ja huomattaessaan saapuvansa WLAN-verkon reuna-alueelle käynnistää client handoff-operaation (KUVIO 6) matkapuhelinverkkoon. Helpottaakseen handoff-prosessia client voi olla myös aktiivisesti yhteydessä sen puheluja välittävään SIP-proxyyn. (Cisco Systems 2007.)

Tämän ratkaisun etuna on se, että se voidaan rakentaa olemassa olevan langattoman verkon päälle, sillä handoff-prosessi painottuu päätelaitteen clientin toimintaan. Ratkaisun yhtenä varjopuolena on se, että jokainen päätelaite vaatii oman client-ohjelmistonsa sekä se tosiasia, että yksittäisten päätelaitteiden handoff-prosessit saattavat toimia arvaamattomasti varsinkin ympäristöissä, joissa liikutaan useiden tukiasemien alueilla. (Cisco Systems 2007.)





KUVIO 9. Clientin toimintaan keskittyvä handoff (Cisco Systems 2007)

Handoff-prosessi voidaan toteuttaa myös kolmen osapuolen kesken, jolloin mukana ovat yrityksen IP-PXB, WLAN-infra sekä clientti. Kun resurssit jakautuvat, saadaan hyvin skaalautuva ratkaisu, jolla pystytään välttämään myös mahdolliset pullonkaulat WLAN-infran tai clientin päässä. Toiminta tällaisessa ratkaisussa perustuu siihen, että WLAN-infra aktiivisesti seuraa laitteen sijaintia verkossa ja handoff-prosessi jaetaan clientin, WLAN-infran sekä IP-PXB:n kesken. (Cisco Systems 2007.)

Päinvastaisessa tapauksessa, siirryttäessä matkapuhelinverkosta yrityksen WLAN-verkon kantaman alueelle, helpoin ratkaisu on olla tekemättä mitään, mikäli clientin päässä on aktiivinen puhelu. Kun käyttäjä sittemmin päättää käynnissä

olevan puhelunsa ja haluaa aloittaa uuden, siirtyy puhelujen ohjaus automaattisesti yrityksen sisäisen VoIP-järjestelmän piiriin. (Cisco Systems 2007.)

#### 4.4 Nokia Call Connect for Cisco

Nokia tarjoaa yritysympäristöihin Nokia Call Connect for Cisco-tuotetta jo valmiisiin Cisco Systemsin, Cisco Unified Communications Manager 4.3 tai sitä uudempiin ratkaisuihin. Call Manager-clientin avulla voidaan integroida esimerkiksi Symbian 60-matkapuhelimia yrityksen puhelininfrastruktuuriin. Puhelimet, joihin tämä tuote asennetaan voivat liikennöidä siitä lähtien niin matkapuhelinverkossa kuin langattomassa VoIP-ympäristössä. (Nokia 2010.)

Tuotteen käyttäjän työntekoa helpottavina ominaisuuksina esitellään muun muassa saman numeron käyttäminen kiinteässä pöytälaitteessa sekä matkapuhelimessa, ilman erillistä puhelunsiirtoa. Verkon sisäisten puhelujen reitittämällä WLAN:iin ylitse, saadaan vähennettyä yrityksen puhelukustannuksia. Matkapuhelimella voidaan myös hallita kiinteän puhelimen ominaisuuksia, kuten puhelujen siirtoa, puhelujen pito ja parkkeeraus ominaisuuksia. Client hoitaa puhelujen roamauksen matkapuhelinverkon ja WLAN-verkon välillä tunnistamalla missä verkossa käyttäjä kulloinkin on. Myös automaattinen rekisteröityminen Call Manageriin on tehty mahdolliseksi. (Nokia 2010.)

Call Connect-tuote on yhteensopiva ainakin Nokia E51, Nokia E52, Nokia E55, Nokia E63, Nokia E66, Nokia E71, Nokia E72, Nokia E75 ja Nokia E90 Communicator puhelinmallien kanssa. Lisäksi Nokia tarjoaa Nokia Intellisync Device Management-ohjelmiston, jonka avulla on mahdollista hallita keskitetysti päätelaitteita, esimerkiksi lukita matkapuhelimen mikäli se häviää tai varastetaan tai sen avulla voidaan siirtää tärkeät tiedot puhelinta vaihdettaessa uuteen laitteeseen. (Nokia 2010.)

Nokia Call Connect for Cisco-tuotteen käyttöönoton hinta riippuu Cisco Call-Managerin versiosta, mutta Call Manager 4:lle, jossa ei ole vielä device-license-pool-lisenssointia hinta on hieman yli 200 euroa. Client itsellään maksaa siis noin 100 euroa ja lisäksi Call Managerin päähän tulee hankkia device-licence-pool-lisenssit. Mikäli organisaatiolla on Call Manager 5 tai sitä uudempi versio, saadaan lisenssejä vapautettua poistuvien laitteiden myötä licence-poolista. Tällaisia laitteita voivat olla esimerkiksi yrityksessä ennestään käytössä olevat Ciscon VoIP-pöytäpuhelimet. Pöytäpuhelinen toiminta saatetaan kokea turhaksi, mikäli matkapuhelimiin otetaan käyttöön Call Connect-clientteja. Tällöin voidaan siirtää pöytäpuhelinen käyttämiä lisenssejä uusille dual-mode-käyttäjille. (Kurkikangas 2009.)

## 5 VARAUTUMINEN TULEVAISUUTEEN

Tulevaisuuden uudistuvat teknologiat tuonevat eteen asioita, jotka tulee ottaa huomioon prosessia valmistellessa. Yksi näistä on IPv6-osoitteistuksen kasvu. Toisaalta IPv6-osoitteet saattavat tuottaa ongelmia, sillä kaikki verkkolaitteet eivät ole yhteensopivia uuden osoitteistusmallin kanssa. Positiivinen tosiasia on, että IPv6-osoitteita on niin paljon, että NAT-muunnosten tekeminen verkossa voidaan kokea turhaksi ja jättää pois käytöstä, mikä taasen helpottaa VoIP-liikennöintiä verkoissa. (Techtarget 2009.)

Pilvitekniikat eli Cloud Computing on nykyaikana kasva trendi. Suomesta on löytynyt jo pitkään toimijoita, jotka tarjoavat yrityksille sekä kuluttajille vuokraympäristöjä. Näiden ympäristöjen kautta voidaan rakentaa uusia verkkoympäristöjä ilman, että ostetaan omia verkkolaitteita. Verkkoympäristöjen ulkoistamiset tuovat kustannustehokkuutta erityisesti pienemmille yrityksille. Yleensä se on verkon ylläpitäjistä kiinni, uskaltavatko he antaa omat lapsensa vieraiden käsiin. (Techtarget 2009.)

Cloud Computing-ympäristöjä tarjoavat yritykset tarjoavat tuotteita muun muassa VoIP, VPN, GSM ja Gateway-ympäristöjen ulkoistamiseen. Tällainen vaihtoehto tulee huomioida, mikäli yrityksessä tulee eteen tilanne, että verkkolaitteita ja tuotteita pitää lähteä uudistamaan. (Techtarget 2009.)

UMA (Universal Mobile Access / Unlicensed Mobile Access) on jossain määrin kasvava mahdollisuus, jossa dual-mode-matkapuhelinta voidaan käyttää useissa eri medioissa. Operaattorit, jotka tukevat UMA:ia, sallivat matkapuhelinpalvelujen käytön julkisissa IP-verkoissa. UMA:ssa idea on, että päätelaitteen yhteydet muodostuvat laajakaistaisen, langattoman verkon kautta aina silloin, kun se vain on mahdollista. UMA voisi tuoda siis langattoman VoIP:n käytön myös työpaikan WLAN-verkon ulkopuolelle. (UMA Today 2009.)

Akun kulutus langatonta VoIP:aa käytettäessä on yksi huomioon otettava tekijä. Tavallisessa mobiiliympäristössä matkapuhelin toimii eri tiloissa. Päätelaitteen status vaihtelee ”sleep”, ”standby”, ”wakes” ja ”talk” tilojen välillä. Näiden eri tilojen kautta voidaan minimoida akun tehonkäyttö. Kun käytössä on langaton media, tulee päätelaitteen olla jatkuvasti kuuntelemassa verkon tapahtumia ja luonnollinen seuraus tälle on suurempi akun kulutus. Akkutekniikat tosin kehittyvät alituisen. IEEE on lisäksi määritellyt 802.11-standardilisäyksen PSM (Power Save Mode), jonka avulla päätelaitteen akunkulutusta voidaan vähentää. Standardi yksin ei kuitenkaan vielä poista ongelmaa vaan sen tueksi kehitellään alati myös muita säästökeinoja. (Anastasi, Conti, Gregori & Passarella 2006.)

## 6 MEDIATALO A-LEHDET

### 6.1 A-lehdet Oy

Yrjö ja Aune Lyytikäinen painoivat kotonaan ensimmäisen Avun vuonna 1933, joka ilmestyi 4000 kappaleen painoksena. Ensimmäisinä vuosinaan Apua jaettiin myytäväksi työttömille, jotka saivat työstään kelpo korvauksen. Vuosien kuluessa yritys kasvoi ja 60-luvulta lähtien Avun rinnalla alettiin kustantaa myös muita lehtiä. Nykyään lehtiä ilmestyy lähemmäs kaksikymmentä. A-lehti Oy:n lisäksi lehtitalossa toimii Image Kustannus, joka julkaisee kolmea lehteä, ja Dialogi, joka toimittaa 30:tä asiakaslehteä. Vuoden 2008 liikevaihto oli 95,0 miljoonaa euroa, ja kaikkiaan A-lehdet Oy työllisti tuolloin 463 henkilöä. (Numminen 2003.)

A-lehtitalo sijaitsee Helsingin Kulosaarella, jossa sillä on 18 lehtitoimitusta, kuvatoimitus, markkinointi-, myynti-, puhelinmyynti- ja talousosastot sekä digitaaliseen mediaan ja julkaisuun keskittyvä osasto. Kaikkiaan työntekijöiden määrä Kulosaarella pyörii kolmen ja puolen sadan paikkeilla, johon voidaan päälle vielä laskea freelancer-toimittajat ja -valokuvaajat. Lisäksi A-lehdillä on yhdeksän omaa puhelinmyyntikonttoria ympäri Suomea ja lisäksi osa puhelinmyynnistä on myyty ulkoisille toimijoille. (Numminen 2003.)

### 6.2 A-lehtitalo Helsingin Kulosaarella

Lehtitalon osastoilla ja toimituksissa työskenteleville henkilöille on jokaisella PC ja / tai Mac-kone, riippuen heidän työtehtävistään. Mac-käyttäjät ovat pääsääntöisesti graafisia suunnittelijoita eli AD:ita, jotka vastaavat lehden

ulkoasusta. Toimittajat sekä muut käyttäjät työskentelevät Windows XP-pohjaisessa pc-maailmassa. Yleinen linjaus on ollut, että paljon raskasta liikennettä siirtävät Macit on kytketty 1 gigan portteihin ja pc-koneet 100 megan portteihin. Vuodelle 2010 on suunnitteilla siirtymistä Windows 7-käyttöjärjestelmiin sekä uudempien palvelinjärjestelmien käyttöönottoa. (Mäkelä 2009.)

Työntekijöille on asennettu Ciscon 79\*\* -sarjan VoIP-pöytäpuhelimet, jotka yleensä toimivat työpisteessä hubin tavoin kuljettaen koneen verkkoliikenteen lävitseen. Osa Ciscon puhelimista on kytketty PoE-kytkimeen (Power over Ethernet), jolloin ulkoisesta virtalähteestä on voitu luopua. Lisäksi työnantaja tarjoaa työntekijöilleen mahdollisuuden hankkia Nokialaisen työpuhelimen, joista suurin osa on jo varustettu WLAN-kortilla. (Mäkelä 2009.)

#### 6.2.1 A-lehtien lähiverkko ja laitteet

A-lehtitalon sisäverkko on, paikallisesti huonoa talokaapelointia lukuun ottamatta, hyvin ajassa mukana. Koko verkko on paloitetu useisiin virtuaalisiin lähiverkkoihin, joista ensimmäiseen on jaettu PC-koneet ja serverit. Mac-koneet on sijoitettu omaan virtuaaliverkkoonsa, kuin myös printterit ja muut pienemmät liikennöijäryhmät. (Mäkelä 2009.)

Eri laitteiden jaottelun lisäksi, myös talon kahdelle langattomalle verkolle löytyy oma VLAN:insa, samoin kuin VPN:lle ja web-palvelimille. Kaikkea verkon liikennettä on verkon reunalla hallinnoimassa Ciscon gateway. (Mäkelä 2009.)

#### 6.2.2 A-lehtien langattomat verkot ja niiden resurssit

Kulosaaren toimipisteeseen on kaksi langatonta verkkoa, joista toinen on avoin ja tarkoitettu talossa vieraileville käyttäjille ja toinen, talon omaan käyttöön

tarkoitettu, suojattu verkko. Tämän suojatun, A-NET:n turvallisuudesta on valittu huolehtimaan WPA Enterprise, TKIP-salauksella ja käyttäjien autentikointi toteutetaan EAP:lla. Langatonta VoIP:ia ajatellen, tulee ottaa huomioon mitä salausten menetelmiä käytettävät päätelaitteet tukevat. Nämä kaksi verkkoa käyttävät samoja Ciscon Lightweight-tukiasemia, mutta ovat kontrollerissa eroteltu kahdeksi eri verkoksi. (Mäkelä 2009.)

Tukiasemia on tällä hetkellä sijoitettuna ympäri taloa 22 kappaletta. Ne on sijoitettu kattamaan rakennuksen eniten käytetyt tilat. Peittoalueen ulkopuolella jäävät vielä parkkihalli, varastot, osa kuvausstudiota ja katvealueitakin löytynee. Lehtitalon langaton verkko ei tällä hetkellä kata koko rakennusta, joten lisää tukiasemia tulee luultavasti hankkia ja verkko mitoittaa uusiksi, jotta saataisiin harkinnassa olevan langattoman VoIP:n käyttöalue optimaaliseksi. (Kurkikangas 2009.)

Uusia tukiasemia sijoitettaessa eri toimituksiin tulee ottaa huomioon ketkä käyttäjät tulisivat käyttämään eniten langatonta verkkoa puhelujen siirtotienä ja missä he liikkuvat. Lisäksi tulee huomioida ruuhkahuiput sekä kuinka paljon yhtäaikaisia puheluita samassa solussa voidaan soittaa. Mikäli langattomien VoIP-käyttäjien osuus jää pieneksi, riittänee että tukiasemien sijoittelu optimoidaan. Mikäli lähdetään rakentamaan langatonta VoIP-infraa kaikille käyttäjille, tulee langattoman verkon kapasiteetti ja rakenne laskea alusta uudelleen. (Kurkikangas 2009.)

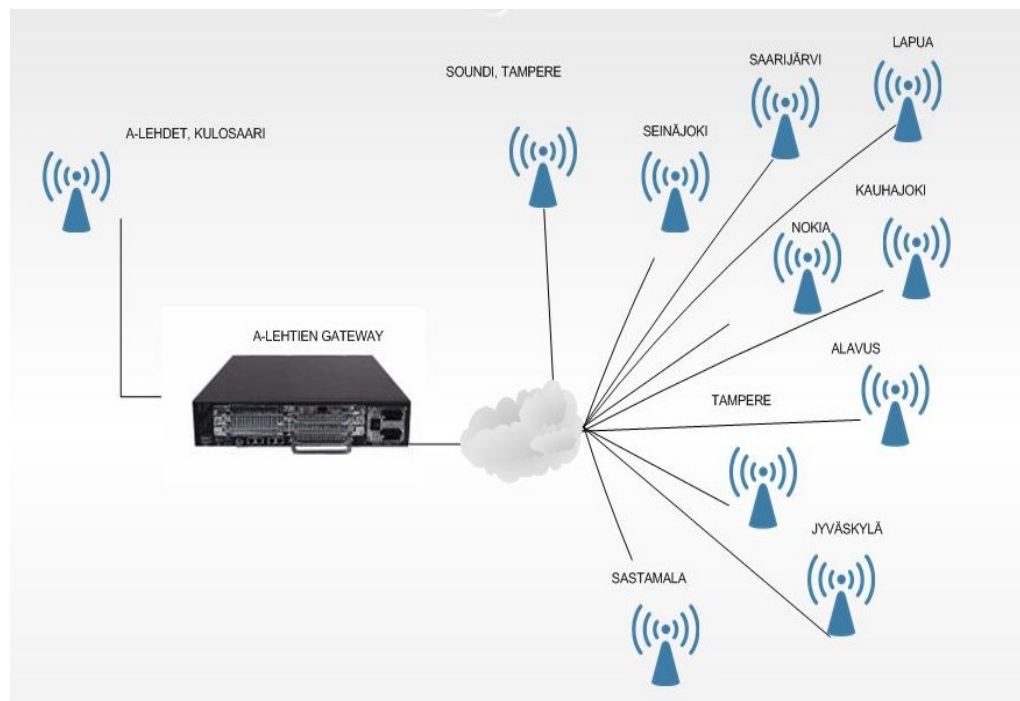
### 6.3 Puhelinmyyntitoimistot ja Soundin toimitus

A-lehdillä on tällä hetkellä yhdeksän omaa puhelinmyyntikonttoria eri paikkakunnilla, joihin kulkee 4 megan yhteys Elisan MPLS-pilven läpi. Jokaisessa konttorissa on myös oma langaton tukiasemansa (KUVIO 10), joka mahdollistaisi langattoman VoIP:n käytön sisäverkon läpi vuoropäälliköiden asioidessa toisiin



konttoreihin tai esimerkiksi teknologiatoimintoon, Helsinkiin.  
(Kurkikangas 2009.)

Puhelinmyyntiin tarkoitettu Occi-soittojärjestelmä on ns. soft-PXB, jota käytetään päätteeltä ja joka hakee sittemmin soittavan numeron GSM-laatikosta, pääkonttorilta. Aiemmin puheluliikenne kulki erikseen kustakin konttorista, mutta nykyään kaikki puhelinmyyntikonttorien puheluliikenne ohjataan Kulosaaren kautta. Occi-järjestelmän liikennetoimintaa ja rakennetta ei tulla muuttamaan ainakaan lähitulevaisuudessa. (Kurkikangas 2009.)



KUVIO 10. A-lehtien langaton verkko (A-lehdet Oy 2009)

Tampereella sijaitseva Soundin toimitus on yhteydessä A-lehtien gatewayhin 100 megan yhteydellä ja on puhelinmyyntikonttorien tavoin yksi loogisen lähiverkon osa. Soundin toimitukseen on myös asennettu WLAN-tukiasema, jonka kautta voitaisiin olla langattomastikin puhelinyhteydessä pääkonttoriin ja muihin yksiköihin. (Kurkikangas 2009.)

## 7 KÄYTTÄJÄTUTKIMUKSIA JA NIIDEN TULOKSIA

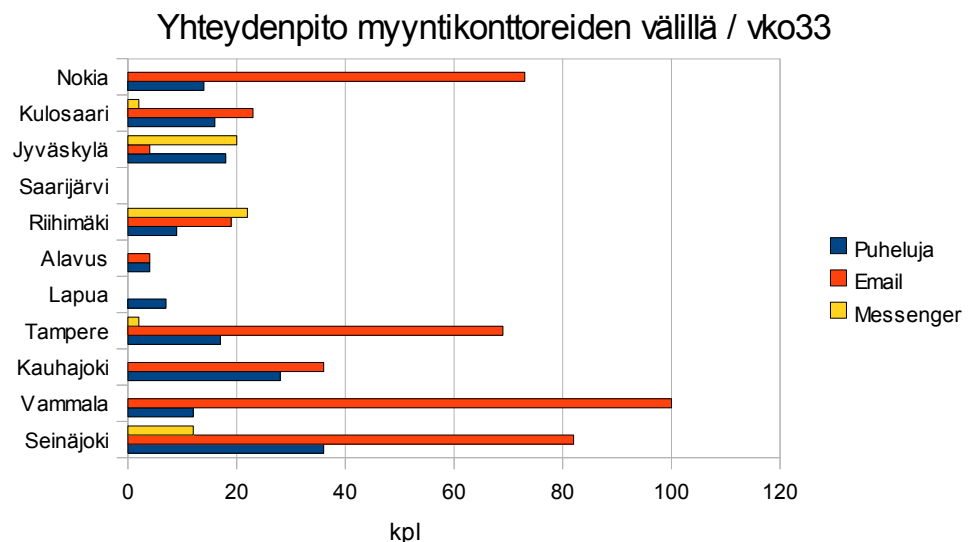
Opinnäytetyötutkimusta varten tehtiin kahdelle A-lehtitalon eri käyttäjäryhmälle käyttäjäkyselyt siitä, miten työntekijät kommunikoivat yrityksen sisällä ja kuinka paljon näitä puheluja on suhteessa talon ulkopuolelle meneviin puheluihin. Kyselyt tehtiin Kulosaaren toimipisteen työntekijöille sekä puhelinkonttorien työntekijöille. (A-lehdet Oy 2009.)

Kulosaaren työntekijöille tehdyssä tutkimuksessa kysyttiin, kuinka suuri osa työpuheluista hoidetaan matkapuhelimilla ja kuinka suuri osa työpisteissä sijaitsevilla Ciscon VoIP-puhelimilla. Käyttäjiltä tiedusteltiin myös tuntevatko he pöytäpuhelimien tarpeelliseksi vai tulisivatko he toimeen pelkästään matkapuhelimilla. Lehtitalon käyttäjä tutkimus julkaistiin yrityksen sisäiseen intraan, Aviisin, jossa kyselylomake oli kaikkien täytettävissä viikon ajan. (A-lehdet Oy 2009.)

Puhelinkonttorien vuorovastaavat ja vuoropäälliköt seurasivat omaa puhelimenkäyttöään viikon verran ja kirjasivat tulokset ylös. Pääkonttorilla teetettiin työntekijöille käyttäytymiskysely yrityksen oman intra-sivuston, Aviisin, kautta. Seuraavissa kappaleissa tutkitaan tutkimustulosten antia ja pohditaan sitä, minkälaisia ratkaisuja saatujen tulosten perusteella kannattaa harkita. (A-lehdet Oy 2009.)

## 7.1 Käyttäjäkyselyn tuloksia puhelinmyyntikonttoreista

A-lehtien puhelinmyyntikonttorien esimiehet ja vuorovastaavat pitivät viikon ajan kirjaa siitä, kehen kollegaansa ja millä tavoin he olivat yhteydessä. Tässä kyselyssä ei otettu kantaa puhelujen kestoihin vaan kirjattiin ylös ainoastaan määriä. Konttorit ovat keskenään päivittäin ahkerasti yhteydessä myynnillisten asioiden merkeissä. Koska kukin myyntikonttori on looginen aliverkkonsa A-lehtien verkossa, voitaisiin kaikki liikenne hoitaa IP-verkossa.



KUVIO 11. Puhelinmyyntikonttoreiden käyttäjäkyselytuloksia (A-lehdet 2009)

Tuloksista (KUVIO 11) käy ilmi, että suurin osa yhteydenpidosta hoidetaan sähköpostilla. Myös osa käyttäjistä käyttää hyväkseen yrityksen sisäistä Windows Messengeriä keskinäiseen yhteydenpitoon. Puheluja tulee kuitenkin viikoittain sadasta viidestäkymmenestä kahteensataan, riippuen sesongista. Puhelujen kestot vaihtelevat viidestä viiteentoista minuuttiin. Näin ollen puhelinkonttorien yrityksen sisäisten puhelujen kustannukset ovat ainakin muutaman sata euroa kuukaudessa. Lisäksi puhelinmyyntikonttorien esimiehet ovat yhteydessä

Kulosaaren puhelinmyynnistä vastaavan toiminnon henkilökuntaan sekä teknologiatoiminnon henkilökuntaan lähes päivittäin.

## 7.2 Käyttäjäkyselyn tuloksia pääkonttorilta

Kulosaaren konttorilla teetettyyn käyttäjätutkimukseen vastanneista (LIITE 1) noin 90 % kertoo, että heidän työpisteeltään löytyy Ciscon 79\*\* -sarjalainen VoIP-puhelin. 40 % näistä käyttäjistä ilmoittaa hoitavansa lähes kaikki yrityksen sisäiset puhelut pöytäpuhelimella. Noin 30 % käyttäjistä ilmoittaa soittavansa vain neljäsosan sisäpuheluistaan pöytäpuhelimella ja loput vastanneista soittaa puolet tai 3/4 sisäpuheluistaan pöytäpuhelimellaan.

Käyttäjän ikä vaikuttaa myös puhelinkäyttäytymiseen. Suurin osa 21 - 35-vuotiaista käyttää enemmän matkapuhelinta kuin pöytäpuhelinta ja tätä vanhemmat käyttäjät pitävät yleisesti enemmän pöytäpuhelimella soittamisesta. Kun käyttäjiltä kysyttiin haluavatko he käyttävät mieluummin matka- vai pöytäpuhelinta työpuheluissaan, 65 % vastanneista soittelee mieluummin matkapuhelimella. Kysyttiin myös olisivatko käyttäjät valmiita siirtymään ainoastaan matkapuhelimen käyttöön, vain 6 vastaajaa 85:ä vastasi kielteisesti.

Käyttäjätutkimustulosten perusteella voidaan todeta, että käyttäjien puhelinkanta on myös suhteellisen tuoretta. Lähes yhdeksällä kymmenestä käyttäjästä käytössä oleva puhelinmalli on E51 tai sitä uudempi. Vain noin 12 % käyttäjistä on käytössään puhelin, joka on malliltaan *'joku vanha nokia'*. E-sarjan E51 puhelimissa ja tätä uudemmissa puhelimissa on WLAN-tuki, joka mahdollistaa langattoman VoIP:n käyttöönoton. Noin 85 % vastanneista käyttää hyväkseen A-lehtien tarjoamaa puhelinetumahdollisuutta, ja mikäli aiempi trendi jatkuu, puhelinmallit uudistuvat jatkuvasti.

Lisäksi tutkimustuloksista nähdään, että käyttäjät jakautuvat puhelujen määrissä ja puhelujen kestoissa. Hieman alle 40 % käyttäjistä soittaa suhteellisen vähän ja

lyhyitä puheluja. Hieman yli 40 % vastanneista ilmoittaa soittavansa 6 - 10 puhelua yhden työpäivän aikana ja että näiden puhelujen kestot vaihtelevat yleensä viiden ja kymmenen minuutin välillä. Loput 20 % vastanneista, tunnustautuvat ahkerammiksi käyttäjiksi. Tämän vähemmistön puhelujen kestot kuitenkin vaihtelevat alle kahden minuutin puheluista yli 10 minuutin mittaisiin puheluihin.

Lähdettäessä kartoittamaan käyttäjiä, joille langaton VoIP olisi taloudellisesti perinteistä GSM-liittymää parempi ratkaisu, on tämän käyttäjätutkimuksen perusteella sellaisia käyttäjiä noin 30 % lehtitalon kaikista työntekijöistä. Prosessia vietäessä eteenpäin, tulee nämä käyttäjät paikallistaa tutkimalla käyttäjien matkapuhelinten laskutusta tarkemmin.

## 8 SKENAARIOITA

Täydellistä käyttäjäkartoitusta toimitusten käyttäjien ja muiden työntekijöiden tarpeista on vaikea tehdä, mutta hyviä suuntaa antavia malleja löydetään. Siinä, miten saatuja käyttäytymismalleja aletaan tutkia, tulee ottaa huomioon, ketkä kaikki tämä tutkimus on oikeasti tavoittanut.

Käyttäjätutkimus julkaistiin A-lehtien intra-sivuilla, jota ahkerimmin seuraavat varmaan ne käyttäjät, jotka työskentelevät pääosin omalla työpisteellään, päätteen vieressä. Liikkuvat työntekijät, jotka tulisivat oikeasti hyötymään langattomuudesta, ovat luultavammin vastanneet tutkimukseen passiivisemmin, ja tämä tulee ottaa huomioon tutkimustuloksia tarkastellessa ja tarvittaessa tehdä vielä tarkempia tutkimuksia yksittäisten käyttäjien puhelinliikenteen käytöstä.

### 8.1 Käyttöönotto puhelinkonttoreiden esimiehille ja yhteyshenkilöille

Eri paikkakunnilla sijaitsevat puhelinkonttorit ovat toisiinsa päivittäin aktiivisesti yhteydessä. Myös Kulosaaren toimipisteeseen ollaan yhteydessä puhelimitse päivittäin. Eri toimipisteiden välistä yhteydenpitoa ja sen kehittämistä pohdittaessa, nousi esiin ajatus näiden henkilöiden välisen liikenteen siirtämisestä langattomaan VoIP:iin. Kiinteät VoIP-puhelimet eivät konttoreiden vuoropäälliköiden ja vuorovastaavien tapauksessa ole hyvä ratkaisu, sillä heidän tulee olla alituisen liikkeellä myyjien tukena eri puolilla toimitiloja.

Jokaisessa konttorissa on jo langaton tukiasemansa. Konttorien langattoman tukiaseman tulee kattaa koko toimitila ja tarvittaessa tulee hankkia useampia laitteita, jotta kattavuus voidaan taata. Vuoropäälliköiden ja vuorovastaavien sekä niiden käyttäjien, jotka kommunikoivat toisiin konttoreihin sekä Helsingin pääkonttoriin, käyttämät puhelinmallit tulee uudistaa sellaisiksi, että ne tukevat

Ciscon VoIP-clientin toimintaa. Tämä ratkaisu on varmasti se ensimmäinen askel, lähdetessä tuomaan langattomuutta A-lehtien VoIP-järjestelmään.

## 8.2 Langattomuutta tarvitsevat käyttäjät – tehokkuutta työntekoon

Sen lisäksi, että vain puhelinkonttoreihin asioivat käyttäjät ottaisivat käyttöön VoIP-clientit matkapuhelimiinsa, on lehtitalon sisällä käyttäjiä, jotka hyötyisivät langattomuudesta. Tällaisia käyttäjiä ovat esimerkiksi kuvausstudiolla työskentelevät valokuvaajat, joiden tarvitsee olla yhteydessä toimituksiin.

Lisäksi osa eri toimintojen työntekijöistä soittaa paljon sisäpuheluita ja he liikkuvat hyvin paljon eri puolilla rakennusta. Tällaisille käyttäjille langaton VoIP voisi tuoda jopa rahallisia säästöjä. Esimerkiksi osa teknologiatoiminnon työntekijöistä liikkuu päivän aikana hyvin paljon eri toiminnoissa ja soittelee suurimmaksi osaksi yrityksen sisäisiä puheluita.

Mikäli lähdetäisiin tarjoamaan osalle Kulosaaren toimipisteen työntekijöistä mahdollisuutta ottaa käyttöön langaton VoIP-ominaisuus matkapuhelimissaan, tulisi langattoman verkon kantama tarkastella uudestaan, jotta voidaan välttää tarpeettomilta hypyiltä langattomasta verkosta mobiiliverkkoon. Tällainen ratkaisu lienee se toinen askel kohti langatonta VoIP-puhelujärjestelmää A-lehtien yrityksessä.

## 8.3 Koko yrityksen muuttaminen langattomaan VoIPpiin

Verkon ylläpitäjän kannalta paras vaihtoehto olisi, että kaikki puheluliikenne liikkuisi samalla lailla ja järjestelmää voidaan hallita yhdestä ja samasta paikasta.

Ajatus siitä, että koko yritystä lähdettäisiin tällä hetkellä muuttamaan langattoman VoIP:n käyttöön, on tällä hetkellä melko kaukainen ajatus. Läheskään kaikkien käyttäjien tarpeet langattomuudelle eivät ole niin suuria, että uusiin laitehankintoihin, tukiasemakapasiteetin kasvattamiseen ja langattoman verkon uudelleen optimoinnin niin suurelle käyttäjämäärälle olisi tarpeellista. Tulevaisuudessa ajatus koko yrityksen langattomuudesta tulee varmasti ajankohtaiseksi.

Suurin projekti, joka tulee toteuttaa ennen kuin voidaan ajatella koko käyttäjämäärän puheluliikenteen siirtämistä langattomaksi, on lehtitalon runkoverkon uudelleenkaapelointi. Langattoman VoIP:n käyttöönoton seurauksena suuresti lisääntyvä liikenteen määrä verkossa vaatii ajanmukaisemman kaapeloinnin. Viimeisten tietojen mukaan A-lehdissä on tällä hetkellä käynnissä muutostyöt talon runkokaapeloinnin uusimiseksi. Askel siirtymän suuntaan on siis jo käynnissä.

#### 8.4 Ratkaisujen toteuttaminen

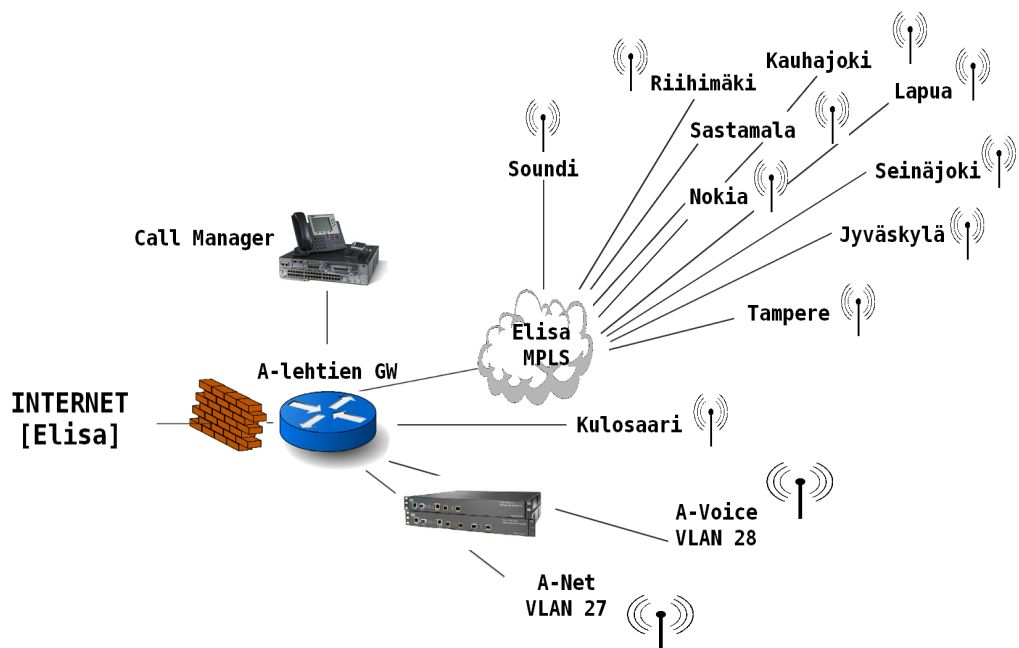
Jokainen ratkaisumalli tultaisiin toteuttamaan jo olemassa olevan VoIP-järjestelmän päälle. Yrityksessä on käytössä Ciscon Systemsin tuotteet, joilla kiinteä VoIP-järjestelmä on nykyisellään toteutettu. Käyttäjämääristä riippuen tullaan kasvattamaan yrityksen langattoman verkon resursseja.

Ratkaisu, jossa otettaisiin langattoman VoIP:n mahdollisuus käyttöön myyntikonttoreissa ja osalle käyttäjistä myös lehtitalon sisällä, ei vaadi sinällään suuria muutoksia verkkoinfraan. Käyttäjien puhelimet tulee tarvittaessa uudistamaa sellaisiksi, että ne tukevat Nokia Call Connect-clienttia ja käyttäjille tulee hankkia kyseinen ohjelmisto näiden puhelimiin. Käyttöpastuksen lisäksi käyttäjien päähän ei tarvitse tehdä muita muutoksia.



Myyntikonttoreita ja Kulosaaren päätoimitilaa yhdistää tällä hetkellä 4 Mbs-yhteydet. Näiden linjojen nopeus tulee tarkastaa ja niitä tulee tarpeen mukaan kasvattaa, mikäli langattoman VoIP:n tuoman verkkoliikenteen katsottaisiin tarvitsevan lisää kapasiteettia.

Call Manager-versio tulee päivittää uudempaan, jotta saadaan tuki toiminnolle, jolla saadaan vapautettua lisenssejä hallintaohjelmiston device-poolista eikä jokaiselle laitteelle näin ollen tarvitse ostaa aina uutta lisenssiä. Lisäksi tukiasemien optimointi tulee suorittaa niin, että niiden toiminta-alue kattaa koko lehtitalon ja myyntikonttoreiden tilat. Signaalointiprotokollaksi tullaan valitsemaan SIP koko verkkoon pääosin SIP:n NAT-ominaisuuksien vuoksi.



KUVIO 12: Uusi ympäristö (A-lehdet, 2010).

Uusiin verkkolaittehankintoihin ei ole välttämätöntä ryhtyä, sillä nykyinen laitteisto on hyvin ajan tasalla. Gatewaylle konfiguroidaan vaaditut määrittelyt ääniliikenteelle VPN:n lävitse ja WLAN-controllerissa luodaan uusi VLAN-verkko ääniliikenteelle langattomassa mediassa.

Nokia Call Connect-tuotetta tukevat puhelimet osaavat käsitellä lähes kaikkia avainnus-, salaus- ja autentikointimenetelmiä, joten A-Voice-verkolle valittavalla salausmenetelmällä ei ole paljoakaan rajoituksia. Esimerkiksi WPA-2 Enterprise EAP-tunnistautumisella on kyseiseen ympäristöön hyvin luotettava ratkaisu.

## 8.5 Siirtymän hyödyt ja haitat vastakkain

Langaton VoIP tuo liikkuvuutta työntekoon. Matkapuhelinten operaattorilähtöiset kustannukset pienenevät, sillä työpaikan sisäiset puhelut liikennöidään yrityksen oman langattoman verkon ylitse. Laitteiden määrää saadaan supistettua, kun työpisteiden kiinteät puhelimet saadaan pois käytöstä. Käytössä olevien kiinteiden VoIP-puhelimet alkavat olla jo iäkkäitä ja näiden vaihtamis- ja huoltokustannukset kasvavat alituisen. Yhtenä painavana tekijänä langaton VoIP tuo myös ulkoiset toimipisteet osaksi järjestelmää. Lisäksi A-lehtien teknologiatoiminnon ylläpitäjien tukipalvelut keskittyvät siirtymän myötä enemmän yhteen.

Langattomaan liikennöintiin siirryttäessä käyttäjän vastuu kasvaa ja heidän kouluttamisensa uuteen käytäntöön on välttämätöntä. Siirtymä tullaan luultavimmin suorittamaan portaittain, jolloin prosessi helpottuu. Matkapuhelinten akkujen kestosta VoIP-käytössä ei ole tarkkoja lukuja, mutta luultavimmin käyttäjät joutuvat lataamaan päätelaitteitaan aiempaa useammin. Hyötyjä ja haittoja siis löytyy. Painavimpina tekijöinä ovat kuitenkin nykyisen VoIP-laitteiston vanheneminen ja laitteiden kasvava uusintapaine sekä ulkoisten toimipisteiden yhdistäminen osaksi VoIP-järjestelmää.

## 9 YHTEENVETO

Opinnäytetyön tavoitteena oli tutkia VoIP-tekniikkaa ja siirtymistä ainakin osittaiseen langattomuuteen A-lehdissä. Opinnäytetyön pohjana on A-lehtitalon verkkoympäristö ja sen käyttäjäkunta. Tutkimus on teoreettinen, eikä siihen sisältynyt käytännönsuutta.

Tutkittiin tarkemmin eri signalointiprotokollien toimintaa ja näiden ominaisuuksia. Todettiin, että SIP-protokolla on NAT-ominaisuuksiltaan H.323-protokollaa edistysellisempi ja näin ollen SIP olisi se protokolla, jonka kautta ääniliikenne saadaan kulkemaan MPLS-pilven lävitse myös ulkopaikkakuntien myyntikonttoreihin.

Tutkittiin tarkemmin, mitä haasteita langattomuus tuo. Työssä tutkittiin, kuinka QoS-palvelut ja tietoturva voidaan taata, minkä lisäksi käsiteltiin eri menetelmiä toteuttaa handoff-prosessi verkon sisällä sekä sisäverkosta ulkoverkkoon. Työssä todettiin QoS-palvelujen takaamisen edellyttävän liikenteen priorisointia, joka toteutetaan erilaisten arvoluokittelujen kautta. Langattomassa verkossa liikennöimisen tietoturvallisuutta kasvatetaan käyttäjien autentikoinnin, liikenteen salauksen ja istuntojen avaimennusten kautta. Handoffin toteuttaminen riippuu lopullisen langattoman verkon resursseista ja siitä, mille verkon laitteelle halutaan antaa suurin vastuu liikenteen hoitamisessa.

Verkkoinfrastruktuurin tarkastelun ja käyttäjätutkimusten perusteella tultiin lopputulokseen, missä ensisijaisin ratkaisumalli olisi osittainen langattoman VoIP:n käyttöönotto. Langaton VoIP kannattaa ensin ottaa käyttöön vain yrityksen myyntikonttoreissa sekä osalle Kulosaaren toimipisteen käyttäjiä. Kokonaisvaltaiselle vaihdokselle ei nähdä vielä tällä hetkellä tarvetta.

Hyötyjä ja haittoja siirtymälle löydetään. Vaikuttavimpina tekijöinä ovat nykyisen VoIP-laitteiston vanheneminen sekä työntekijöiden liikkuvuden tarve ja toisaalta siirtymään liittyvän käyttäjien koulutuksen ja Nokia Call Connect-lisenssien tuomat kustannukset.

Tulevaisuudessa tullaan tienristeykseen, jossa päätös on tehtävä siitä, investoidaanko kokonaisvaltaiseen langattomaan VoIP-järjestelmään, ostetaanko uusia kiinteän VoIP-järjestelmän laitteita vai pystyykö kentien operaattori tai muu ulkoinen toimija tarjoamaan vastaavanlaisen järjestelmän ulkoistettuna palveluna. Langattomuus on tulevaisuuden trendi lähes kaikkien alojen yrityksissä. Mobiilius ja tehokkuus ovat rahanarvoisia tekijöitä työmaailmassa ja langaton VoIP on yksi nämä tekijät mahdollistava tekniikka. VoIP-toimintojen ulkoistaminen ja palveluntarjoajien määrien kasvaminen ovat myös todennäköisiä tulevaisuuden trendejä yrityksissä.

## LÄHTEET

A-lehdet Oy. 2009. Käyttäjätutkimus Kulosaaren toimitilojen työntekijöille 21.8.2009 [viitattu 10.2.2010].

Anastasi, G., Conti, M., Gregori, E. & Passarella, A. 2007. 802.11 power-saving mode for mobile computing in Wi-Fi hotspots: Limitations, enhancements and open issues. Springer Netherlands [viitattu 10.2.2010]. Saatavissa: <http://www.springerlink.com/content/4673x17044513p24/>

Cisco Systems. 2004. Call Manager version 4. Cisco Systems [viitattu 1.3.2010]. Saatavissa: [http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_data\\_sheet09186a00801f8e2e.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_data_sheet09186a00801f8e2e.html)

Cisco Systems 2007. Seamless Roaming for Enterprises. Cisco Systems [viitattu 20.11.2009]. Saatavissa: [http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns789/white\\_paper\\_c11-504030.html](http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns789/white_paper_c11-504030.html)

Cisco Systems. 2008. Unified Communications over WLAN Solution Overview. Cisco systems [viitattu 10.8.2009] Saatavissa: [http://www.cisco.ag/en/US/solutions/collateral/ns340/ns394/ns348/solution\\_overview\\_c22-476919.pdf](http://www.cisco.ag/en/US/solutions/collateral/ns340/ns394/ns348/solution_overview_c22-476919.pdf)

Cisco Systems. 2009. SP Hosted NAT Traversal for SIP Calls Using Cisco IOS Session Border Controller. Cisco Systems [viitattu 19.1.2010]. Saatavissa: [http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6640/prod\\_white\\_paper0900aecd80537d0b.html](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6640/prod_white_paper0900aecd80537d0b.html)

Configuring SIP Connection-Oriented Media, Forking, and MLPP Features. 2007. Cisco Systems [viitattu 15.2.2010]. Saatavissa: [http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip\\_cg-com\\_fork\\_mlpp.html#wp2045945](http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-com_fork_mlpp.html#wp2045945)

Goldman, J. 2008. Introducing IEEE 802.11r. Wi-Fi Planet [viitattu 3.10.2009]. Saatavissa: <http://www.wi-fiplanet.com/news/article.php/3776351>

Griffith, E. 2004. 802.11i Security Specification Finalized. Wi-Fi Planet [viitattu 10.8.2009]. Saatavissa: <http://www.wi-fiplanet.com/news/article.php/3373441>

H.323 Standards. 2002. H.323 Forum [viitattu 20.1.2010]. Saatavissa: <http://www.h323forum.org/standards/>

Hintikka, K. 2004. VoIP over WLAN. Helsinki: TKK [viitattu 25.7.2009]. Diplomityö. Saatavissa: [https://www.netlab.tkk.fi/opetus/s38310/03-04/kalvot03-04/Hintikka\\_010604.ppt](https://www.netlab.tkk.fi/opetus/s38310/03-04/kalvot03-04/Hintikka_010604.ppt)

Hyttinen, J. 2001. VoIP-yhdystkäytävä. Lappeenranta: Lappeenrannan TKK [viitattu 25.7.2009]. Diplomityö. Saatavissa: <https://oa.doria.fi/bitstream/handle/10024/34438/nbnfi-fe20021026.pdf?sequence=1>

Kurkikangas, T. 2009. IT-palvelupäällikkö. A-lehdet Oy. Haastattelu 25.7.2009.

Lakas, A. & Boulmalf, M. 2005. Study of Effect of Mobility Handover on VoIP over WLAN. College of Information Technology, UAE University [viitattu 10.1.2010]. Saatavissa: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04085441>

Magalhaes, R. 2005. Session Initiation Protocol (SIP) and Its Functions. Windows Networking [viitattu 29.12.2009]. Saatavissa: [http://www.windowsnetworking.com/articles\\_tutorials/Session-Initiation-Protocol-Functions.html](http://www.windowsnetworking.com/articles_tutorials/Session-Initiation-Protocol-Functions.html)

Mäkelä, J. 2009. Järjestelmäasiantuntija. A-lehdet Oy. Haastattelu 15.8.2009.

Nokia. 2010. Nokia Call Connect for Cisco. Nokia [viitattu 25.2.2010]. Saatavissa: <http://europe.nokia.com/find-products/nokia-for-business/software/advanced-voice-and-conferencing/nokia-call-connect-for-cisco>

Numminen, J. 2003. Tarina A-lehtitalosta. A-lehdet Oy. Keuruu: Otavan Kirjapaino Oy.

Packetizer. 2009. Understanding SIP-Based VoIP. Packetizer, Inc. [viitattu 22.10.2009]. Saatavissa: [http://www.packetizer.com/ipmc/sip/papers/understanding\\_sip\\_voip/sip\\_call\\_flow.png](http://www.packetizer.com/ipmc/sip/papers/understanding_sip_voip/sip_call_flow.png)

Phifer, L. 2005. When quality counts: 802.11e, WMM, and beyond. SearchMobileComputing.com [viitattu 7.8.2009]. Saatavissa: <http://searchmobilecomputing.techtarget.com/tip/When-quality-counts-80211e-WMM-and-beyond>

Plewes, A. 2007. VoIP security - VoIP threats to watch out for. Silicon [viitattu 20.7.2009]. Saatavissa: <http://www.silicon.com/legacy/research/specialreports/voipsecurity/0,3800013656,39166244,00.htm>

Puska, M. 2005. Langattomat lähiverkot. Helsinki: Talentum Media Oy

Rosenberg, J., Schulzrinne, H. 2002. SIP: Session Initiation Protocol. IETF.org [viitattu 17.10.2009]. Saatavissa: <http://tools.ietf.org/html/rfc3261>

Savonia ammattikorkeakoulu. 2007. Tietoturva. Savonia [viitattu 20.2.2009]. Saatavissa: [http://wirelessplatform.savonia.fi/index.php?option=com\\_content&task=view&id=35&Itemid=59](http://wirelessplatform.savonia.fi/index.php?option=com_content&task=view&id=35&Itemid=59)

Snyder, J. 2002. What is 802.1x?. Networkworld [viitattu 27.9.2009]. Saatavissa: <http://www.networkworld.com/research/2002/0506whatisit.html>

Taavila, Erik. 2008. WLAN turvallisuus. Lappeenrannan teknillinen yliopisto. Saatavissa: [http://www.slidefinder.net/W/WLAN\\_turvallisuus\\_Erik\\_Taavila\\_TiTe/9917224](http://www.slidefinder.net/W/WLAN_turvallisuus_Erik_Taavila_TiTe/9917224)

Techtarget. 2009. Cloud Computing. Techtarget [viitattu 20.1.2010]. Saatavissa: [http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201\\_gci1287881,00.html](http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1287881,00.html)

Tittel, E. 2001. Using H.323 with NAT. Searchnetworking [viitattu 15.2.2010]. Saatavissa: [http://searchnetworking.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid7\\_gci782072,00.html](http://searchnetworking.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid7_gci782072,00.html)

UMA Today 2009. Uma Overview. Uma Today [viitattu 20.1.2010]. Saatavissa: <http://www.umatoday.com/umaOverview.php>

VoIP. 2009. Voip Business Solutions [viitattu 22.7.2009]. Saatavissa: <http://www.voipbusiness.us/voip/>



Voip Network Components. 2009. VoIP-Voice-over-IP.com [viitattu 12.1.2010].

Saatavissa: <http://www.voip-voice-over-ip.com/technology/components.htm>

Voipforo. 2007. H.323 Example. Voipforo [viitattu: 17.10.2009]. Saatavissa:

[http://www.voipforo.com/en/H323/H323\\_example.php](http://www.voipforo.com/en/H323/H323_example.php)

Wallingford, T. 2005. Switching to VoIP. Sebaslitopol: O'Reilly Media.

Wierenga, K. 2009. IEEE 802.11u Overview. Cisco Systems [viitattu 5.11.2009].

Saatavissa: <http://www.terena.org/activities/tf-mobility/meetings/19/wierenga-802.11u.pdf>

Wi-Fi Planet. 2005. 8021x-fig1.jpg. Wi-Fi Planet [viitattu 28.1.2010].

Saatavissa: <http://www.wi-fiplanet.com/img/8021x-fig1.jpg>

## LIITTEET

## LIITE 1 / 1

Vastaaja	Ikä	Toiminto / toimitus	Puh / pvä
1	21-27	IT	6-10
2	36-45	Apu	6-10
3	36-45		Alle 5
4	46-55	Markkinointi	6-10
5	21-27	Digit. Markkinointi	Alle 5
6	36-45	Asiakastiedonhallinta	6-10
7	46-55	Repro	6-10
8	46-55	Taloushallinto	6-10
9	36-45	Puhelinmarkkinointi	Alle 5
10	36-45	IT	Alle 5
11	29-35	Dialogi	6-10
12	46-55	Kuvatoimitus	11-20
13	36-45	Taloushallinto	6-10
14	21-27	Dialogi	Alle 5
15	29-35	Asiakastiedonhallinta	Alle 5
16	29-35	Dialogi	6-10
17	46-55	Viherpiha	Alle 5
18	36-45	Taloushallinto	Alle 5
19	21-27	Avotakka	Alle 5
20	56-65	Mediamyynti	11-20
21	29-35	Puhelinmarkkinointi	6-10
22	36-45	IT	11-20
23	56-65		11-20
24	36-45	Tilausliikenne	Alle 5
25	29-35	Image	Alle 5
26	29-35	Tilausliikenne	Alle 5
27	36-45	Markkinointi	11-20
28	36-45	Mediamyynti	11-20
29	29-35	Suoramarkkinointi	Alle 5
30	29-35	Lehtien myynti ja markkinointi	Alle 5
31	46-55	Irtotilamyynti	6-10
32	36-45	Lehtien myynti ja markkinointi	6-10
33	36-45	Kuva- ja logistiikkapalvelut	11-20
34	56-65	Suoramarkkinointi	6-10
35	36-45	Omat myyntitoimistot	6-10
36	29-35	IT	Alle 5
37	36-45	Markkinointi	6-10
38	29-35	Markkinointi	6-10
39	56-65		Alle 5
40	36-45	Ilmoitusmyynti	11-20
41	56-65	Taloushallinto	6-10
42	36-45	K&T	6-10
43	36-45	Tilausliikenne	Alle 5
44	29-35	Mondo	11-20
45	46-55	Jade	Alle 5
46	46-55	Suoramarkkinointi	6-10
47	21-27	Digimedia	Alle 5
48	29-35	IT	6-10
49	46-55		6-10
50	36-45	Maku	6-10
51	46-55	Lehtien myynti ja markkinointi	6-10
52	36-45	Mediamyynti	11-20
53	56-65	Kuvatoimitus	Alle 5
54	46-55	Henkilöstötoiminto	6-10
55	36-45	Dialogi	6-10
56	36-45	Johto	11-20
57	46-55	Asiakastiedonhallinta	Alle 5
58	56-65	Mediamyynti	6-10
59	46-55	IT	6-10
60	29-35	Asiakastiedonhallinta	Alle 5
61	46-55	IT	Alle 5
62	21-27	Demi	6-10
63	46-55	Tilausliikenne	Alle 5
64	29-35	Avotakka	11-20
65	36-45	IT	6-10
66	29-35	Digimedia	Alle 5
67	29-35	Digimedia	Alle 5
68	36-45	Mediamyynti	6-10
69	46-55	Puhelinmarkkinointi	6-10
70	36-45	Dialogi	6-10
71	46-55	Tilausliikenne	6-10
72	56-65	Apu	11-20
73	36-45	Repro	Alle 5
74	29-35	Avotakka	Alle 5
75	29-35	Demi	Alle 5
76	29-35	Tuulilasi	Alle 5
77	36-45	Mediamyynti	11-20
78	36-45	Henkilöstötoiminto	6-10
79	46-55	Mediamyynti	11-20
80	46-55	Markkinointi	6-10
81	36-45	Digimedia	Alle 5
82	46-55	Meidän Mökki	Alle 5
83	36-45	Viherpiha	Alle 5
84	29-35	Tuulilasi	11-20
85	29-35	IT	6-10

## LIITE 1. Käyttäjätutkimustulokset

## LIITE1 / 2

Vastaaja	Keskim. Kesto / Puh	Talon sis. Puheluita	Ciscon pöytäpuhelin
1	3 – 5 min	10%	Kyllä
2	3 – 5 min	25%	Kyllä
3	Alle 2 min	10%	Kyllä
4	Alle 2 min	10%	Kyllä
5	3 – 5 min	50%	Kyllä
6	Alle 2 min	25%	Kyllä
7	Alle 2 min	75%	Kyllä
8	3 – 5 min	50%	Kyllä
9	3 – 5 min	50%	Kyllä
10	Alle 2 min	75%	Kyllä
11	3 – 5 min	<10%	Ei ole
12	3 – 5 min	50%	Kyllä
13	3 – 5 min	50%	Kyllä
14	3 – 5 min	Alle 10%	Ei ole
15	3 – 5 min	Lähes kaikki	Kyllä
16	Alle 2 min	50%	Ei ole
17	3 – 5 min	75%	Kyllä
18	3 – 5 min	25%	Kyllä
19	Alle 2 min	25%	Kyllä
20	3 – 5 min	50%	Kyllä
21	3 – 5 min	75%	Kyllä
22	Alle 2 min	75%	Kyllä
23	Alle 2 min	10%	Ei ole
24	3 – 5 min	Lähes kaikki	Kyllä
25	3 – 5 min	Alle 10%	Kyllä
26	3 – 5 min	50%	Kyllä
27	6 – 10 min	23%	Kyllä
28	3 – 5 min	Alle 10%	Kyllä
29	Alle 2 min	Alle 10%	Kyllä
30	3 – 5 min	75%	Kyllä
31	3 – 5 min	75%	Kyllä
32	Yli 10 min	Alle 10%	Kyllä
33	3 – 5 min	50%	Kyllä
34	Alle 2 min	10%	Ei ole
35	3 – 5 min	Alle 10%	Kyllä
36	6 – 10 min	75%	Kyllä
37	3 – 5 min	75%	Kyllä
38	6 – 10 min	25%	Kyllä
39	Alle 2 min	Alle 10%	Ei ole
40	6 – 10 min	10%	Kyllä
41	3 – 5 min	75%	Kyllä
42	3 – 5 min	50%	Kyllä
43	Alle 2 min	50%	Kyllä
44	3 – 5 min	Alle 10%	Kyllä
45	3 – 5 min	50%	Kyllä
46	3 – 5 min	Alle 10%	Kyllä
47	3 – 5 min	Alle 10%	Kyllä
48	3 – 5 min	Lähes kaikki	Kyllä
49	6 – 10 min	10%	Kyllä
50	6 – 10 min	50%	Kyllä
51	3 – 5 min	Alle 10%	Kyllä
52	Yli 10 min	50%	Kyllä
53	3 – 5 min	Lähes kaikki	Ei ole
54	3 – 5 min	75%	Kyllä
55	6 – 10 min	Alle 10%	Ei ole
56	3 – 5 min	Alle 10%	Kyllä
57	3 – 5 min	25%	Kyllä
58	3 – 5 min	10%	Kyllä
59	Alle 2 min	50%	Kyllä
60	3 – 5 min	25%	Kyllä
61	3 – 5 min	50%	Kyllä
62	3 – 5 min	25%	Kyllä
63	3 – 5 min	25%	Kyllä
64	6 – 10 min	Alle 10%	Kyllä
65	3 – 5 min	Lähes kaikki	Kyllä
66	3 – 5 min	Lähes kaikki	Kyllä
67	3 – 5 min	75%	Kyllä
68	3 – 5 min	50%	Kyllä
69	3 – 5 min	75%	Kyllä
70	Yli 10 min	25%	Ei ole
71	3 – 5 min	50%	Kyllä
72	3 – 5 min	50%	Kyllä
73	Alle 2 min	Lähes kaikki	Ei ole
74	3 – 5 min	50%	Kyllä
75	3 – 5 min	75%	Kyllä
76	6 – 10 min	Alle 10%	Kyllä
77	3 – 5 min	25%	Kyllä
78	Yli 10 min	75%	Kyllä
79	3 – 5 min	25%	Kyllä
80	6 – 10 min	50%	Kyllä
81	3 – 5 min	25%	Ei ole
82	6 – 10 min	Alle 10%	Kyllä
83	6 – 10 min	25%	Kyllä
84	Alle 2 min	50%	Kyllä
85	Alle 2 min	Lähes kaikki	Kyllä

## LIITE 1 / 3

Vastaaja	Sisäpuh. Osuus pöytäpuhelimella	Puhelinetu	Puhelimen malli
1	10%	Ei	
2	Lähes kaikki	Kyllä	E51
3	Alle 10%	Kyllä	E51
4	10%	Ei	
5	75%	Kyllä	E51
6	Lähes kaikki	Kyllä	E71
7	75%	Ei	
8	50%	Kyllä	?
9	50%	Ei	
10	Lähes kaikki	Kyllä	E70
11		Kyllä	<E51
12	Alle 10%	Kyllä	E51
13	50%	Kyllä	E71
14		Kyllä	E51
15	Lähes kaikki	Kyllä	E51
16		Kyllä	E51
17	75%	Kyllä	<E51
18	25%	Ei	
19	50%	Kyllä	E51
20	50%	Kyllä	E71
21	Lähes kaikki	Kyllä	E51
22	Lähes kaikki	Kyllä	E51
23		Kyllä	E75
24	Lähes kaikki	Ei	
25	Lähes kaikki	Kyllä	<E51
26	50%	Kyllä	E51
27	Lähes kaikki	Kyllä	E51
28	Lähes kaikki	Kyllä	E61i
29	25%	Kyllä	E51
30	Lähes kaikki	Kyllä	E51
31	Lähes kaikki	Kyllä	E51
32	Alle 10%	Kyllä	E51
33	50%	Kyllä	E71
34		Kyllä	E51
35	Lähes kaikki	Kyllä	E61i
36	Lähes kaikki	Kyllä	E51
37	Lähes kaikki	Kyllä	E51
38	75%	Kyllä	E61i
39		Kyllä	E51
40	10%	Kyllä	E61i
41	75%	Kyllä	E71
42	75%	Kyllä	E71
43	75%	Kyllä	E51
44	10%	Ei	
45	Lähes kaikki	Kyllä	E71
46	25%	Kyllä	<E51
47	Alle 10%	Kyllä	E71
48	75%	Kyllä	E55
49	25%	Kyllä	E71
50	50%	Kyllä	<E51
51	Lähes kaikki	Kyllä	E90
52	75%	Kyllä	E51
53		Kyllä	<E51
54	75%	Kyllä	E51
55	Alle 10%	Kyllä	E65
56	Alle 10%	Kyllä	E71
57	Lähes kaikki	Kyllä	E71
58	50%	Kyllä	E71
59	25%	Kyllä	E90
60	Lähes kaikki	Kyllä	E50
61	Lähes kaikki	Kyllä	E75
62	25%	Ei	
63	25%	Ei	
64	Alle 10%	Kyllä	E51
65	Lähes kaikki	Kyllä	N78
66	Lähes kaikki	Kyllä	E51
67	Lähes kaikki	Kyllä	E71
68	25%	Kyllä	<E51
69	Alle 10%	Kyllä	E90
70		Kyllä	E51
71	Lähes kaikki	Kyllä	E71
72	Lähes kaikki	Kyllä	N70
73		Ei	
74	Lähes kaikki	Kyllä	E51
75	75%	Ei	
76	50%	Kyllä	E51
77	75%	Kyllä	E71
78	75%	Kyllä	E61i
79	Lähes kaikki	Ei	
80	Lähes kaikki	Kyllä	<E51
81		Kyllä	E51
82	Alle 10%	Kyllä	<E51
83	Lähes kaikki	Kyllä	<E51
84	Lähes kaikki	Kyllä	E51
85	Lähes kaikki	Kyllä	HTC Touch Pro

## LIITE 1 / 4

Vastaaja	Sisäpuh. Osuus matkapuhelimella	GSM vs. Pöytä	Toimeen vain matkapuhelimella
1	25%	GSM	Kyllä
2	50%	GSM	Kyllä
3	Ei GSM puh	GSM	Kyllä
4	Ei GSM puh	Pöytä	Kyllä
5	10%	Pöytä	Kyllä
6	75%	GSM	Kyllä
7	Alle 10%	Pöytä	Kyllä
8	10%	Pöytä	Kyllä
9	Alle 10%	Pöytä	Kyllä
10	Ei GSM puh	Pöytä	Kyllä
11	Alle 10%	GSM	Kyllä
12	75%	GSM	Kyllä
13	10%	Pöytä	Kyllä
14	Lähes kaikki	GSM	Kyllä
15	Alle 10%	GSM	Kyllä
16	Lähes kaikki	GSM	Kyllä
17	25%	Pöytä	Kyllä
18	Ei GSM puh	Pöytä	Kyllä
19	Ei GSM puh	GSM	Kyllä
20	10%	Pöytä	Kyllä
21	50%	GSM	Kyllä
22	50%	GSM	Kyllä
23	Ei GSM puh	GSM	Kyllä
24	Ei GSM puh	Pöytä	Ei
25	Ei GSM puh	GSM	Kyllä
26	Alle 10%	Pöytä	Kyllä
27	Alle 10%	GSM	Kyllä
28	Ei GSM puh	GSM	Kyllä
29	10%	Pöytä	Kyllä
30	Alle 10%	Pöytä	Kyllä
31	25%	GSM	Kyllä
32	50%	GSM	Kyllä
33	75%	GSM	Kyllä
34	25%	GSM	Kyllä
35	25%	GSM	Kyllä
36	10%	GSM	Kyllä
37	50%	GSM	Kyllä
38	50%	GSM	Kyllä
39	50%	GSM	Kyllä
40	Alle 10%	Pöytä	Kyllä
41	10%	GSM	Kyllä
42	Alle 10%	GSM	Kyllä
43	Alle 10%	Pöytä	Kyllä
44	Ei GSM puh	Pöytä	Ei
45	75%	GSM	Kyllä
46	Alle 10%	Pöytä	Kyllä
47	Lähes kaikki	GSM	Kyllä
48	50%	GSM	Kyllä
49	75%	GSM	Kyllä
50	50%	GSM	Kyllä
51	Lähes kaikki	GSM	Kyllä
52	25%	Pöytä	Kyllä
53	25%	GSM	Kyllä
54	Ei GSM puh	Pöytä	Kyllä
55	Alle 10%	GSM	Kyllä
56	50%	GSM	Kyllä
57	75%	GSM	Kyllä
58	25%	GSM	Kyllä
59	50%	GSM	Kyllä
60	50%	GSM	Kyllä
61	Alle 10%	GSM	Kyllä
62	Ei GSM puh	Pöytä	Kyllä
63	Ei GSM puh	Pöytä	Ei
64	10%	Pöytä	Ei
65	Alle 10%	Pöytä	Kyllä
66	50%	GSM	Kyllä
67	50%	GSM	Kyllä
68	75%	GSM	Kyllä
69	75%	GSM	Kyllä
70	75%	GSM	Kyllä
71	Ei GSM puh	GSM	Kyllä
72	10%	Pöytä	Kyllä
73	Ei GSM puh	Pöytä	Kyllä
74	Ei GSM puh	GSM	Kyllä
75	Alle 10%	Pöytä	Ei
76	50%	GSM	Kyllä
77	50%	GSM	Kyllä
78	Ei GSM puh	GSM	Kyllä
79	25%	Pöytä	Ei
80	50%	GSM	Kyllä
81	Alle 10%	GSM	Kyllä
82	Ei GSM puh	GSM	Kyllä
83	Ei GSM puh	GSM	Kyllä
84	Lähes kaikki	GSM	Kyllä
85	50%	Pöytä	Kyllä